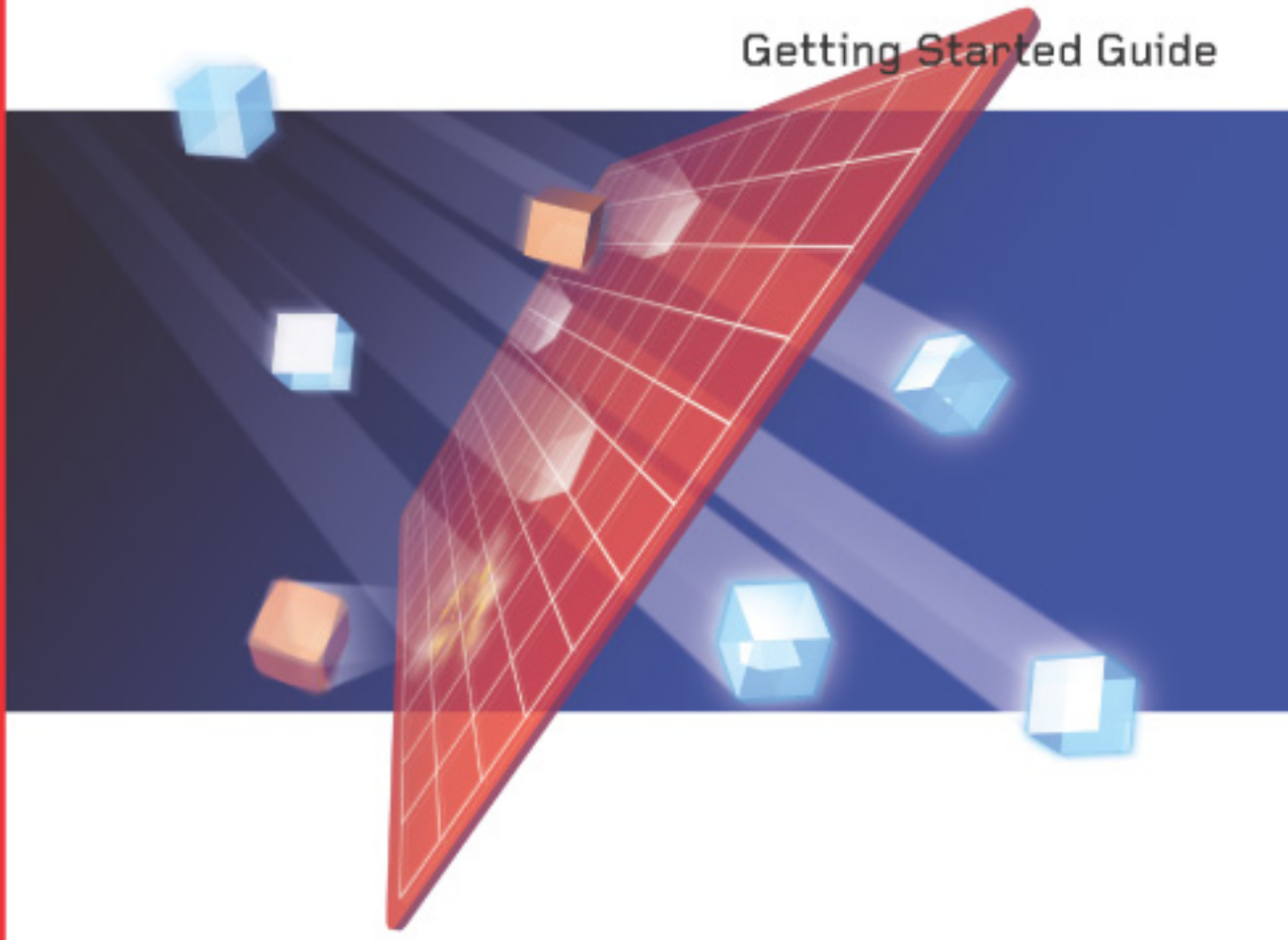
TREND MICRO™

InterScan™ 5 Messaging Security Suite

Comprehensive Security for the Messaging Gateway

for Solaris™/Linux™

Getting Started Guide



TREND MICRO™

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, review the readme files, release notes, and the latest version of the Getting Started Guide, which are available on Trend Micro's Web site at:

http://www.trendmicro.com/download

NOTE: A license to Trend Micro antivirus software includes the right to receive Pattern File Updates and Product Updates and technical support for one (1) year. A license to Trend Micro™ Spam Prevention Solution includes the right to receive Product Updates and local basic technical support for one (1) year from the date of purchase. Thereafter, you must renew Maintenance on an annual basis by paying Trend Micro's then-current Maintenance fees to have the right to continue receiving product updates, pattern updates and basic technical support.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

http://www.trendmicro.com/en/purchase/license/license.htm

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). For more information, see the online help system within the InterScan MSS Web-based management console.

This product uses code from the DMC TextFilter Ver. 3.2 Copyright 1999-2002 Antenna House, Inc.

Document Part No. MSEM51380/30620

Release Date: October 2005

Protected by U.S. Patent No. 5,951,698 and 5,623,600

The Getting Started Guide for Trend Micro™ InterScan™ Messaging Security Suite 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 online SolutionBank at Trend Micro's Web site. For information on troubleshooting or contacting Trend Micro, see *Troubleshooting and Contact Information* starting on Page 9-1.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Standards References

InterScan MSS is built on and is compatible with the following Internet standards:

SMTP : 2821, 2822, 2505, 1869, 1870, 1891, 1652
MIME: 2045, 2046, 2047, 2048, 2049
DNS: 1034, 1035
POP: 1939, 1734, 2449

Contents

Chapter 1

Introducing InterScan™ MSS

InterScan™ Messaging Security Suite (IMSS) is a comprehensive antivirus and content management solution for the Internet mail gateway. It is a functional SMTP server that analyzes the content of messages before sending them to their final destination.

This chapter explains the virus and email content threats that InterScan MSS can stop at the SMTP gateway and introduces the program's key services:

- Antivirus protection
- Content management
- Anti-spam protection
- Protection against other email threats
- Monitoring the SMTP gateway
- Mass mailing virus containment
- Email policies

InterScan MSS main features

InterScan MSS protects your network from virus infection through the SMTP gateway. In addition, the eManager™ content filtering provides intelligent message content management to ensure the integrity of your messaging system.

The following describes the main features of InterScan MSS:

Antivirus protection

InterScan MSS uses the Trend Micro scan engine and a process called pattern matching to detect viruses. The scan engine uses a virus pattern to compare files travelling through your gateway with patterns of known viruses. If the scan engine detects a virus, it can be configured to clean the file by removing the virus code. Trend Micro releases new virus pattern files as new viruses are identified by TrendLabs.

In addition, Microsoft® Office® files are scanned with Trend Micro MacroTrap™. MacroTrap detects macro viruses by analyzing the macro code in Microsoft Office files to detect virus-like behavior.

Content management

InterScan MSS analyzes email messages and their attachments travelling to and from your network for appropriate content. IMSS can effectively block or defer content that you deem inappropriate, such as personal communication, large attachments, and so on.

Spam filtering

With the integration of the Trend Micro Spam Prevention Solution's heuristic filtering technology, InterScan MSS also provides spam-filtering capabilities, using rules to identify spam.

Protection against other email threats

InterScan MSS protects against the following threats to your company's messaging system:

Email Denial of Service (DoS) Attacks

By flooding a mail server with large attachments, or sending messages that contain multiple viruses or recursively-compressed files, malicious individuals can disrupt mail processing. InterScan MSS allows you to configure the characteristics of messages that you want to stop at the SMTP gateway, thus reducing the chances of a DoS attack.

Malicious email content

Many types of file attachments, such as executable programs and documents with embedded macros, can harbor viruses. Messages with HTML script files, HTML links, Java applets, or ActiveX controls can also perform harmful actions. InterScan MSS allows you to configure the types of messages that to allow through the SMTP gateway.

Degradation of services

Non-business-related email traffic has become a problem in many organizations. Spam messages consume network bandwidth and affect employee productivity. Some employees use company messaging systems to send personal messages, transfer large multimedia files, or conduct personal business during working hours.

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

Legal liability and business integrity

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

InterScan MSS provides tools for monitoring and blocking content that help reduce the risk of messages containing inappropriate or confidential material passing through your gateway.

Monitoring the SMTP gateway

InterScan MSS's System Monitor informs administrators at the first sign of mail processing issues. Detailed logging helps administrators proactively manage issues before problems arise.

Mass-mailing virus containment

Email-borne viruses that automatically spread bogus messages through a company's messaging system can be expensive to clean up and cause panic among users. For this reason, when InterScan MSS detects a mass-mailing virus, the action taken against this virus can be different from the actions against other types of viruses.

For example, if InterScan MSS detects a macro virus in a Microsoft Office document with important information, you can configure the program to quarantine the message instead of deleting the entire message, to ensure that important information will not be lost. However, if InterScan MSS detects a mass-mailing virus, the program can automatically delete the entire message to avoid using server resources to scan, quarantine, or otherwise process messages and files that have no redeeming value.

The identities of known mass-mailing viruses are in the virus pattern files that are updated using the TrendLabs™ Active Update servers. You can save resources, avoid help desk calls from concerned employees and eliminate post-outbreak cleanup work by choosing to automatically delete these types of viruses and their email containers.

What's New

Trend Micro Network Reputation Service

InterScan MSS now provides a platform for Trend Micro Network Reputation Service, an IP-level spam filtering product (licensed separately), which blocks unwanted messages, including spam and directory harvest attacks, at the gateway—before it enters your network.

Centralized spam reporting

For users who have licensed Trend Micro Spam Prevention Solution (SPS), InterScan™ Messaging Security Suite provides centralized spam reporting across all local servers hosting IMSS, in conjunction with a database.

Web-based end user quarantine

The Web-based end user spam quarantine feature, for users who have licensed Trend Micro Spam Prevention Solution (SPS), provides Web-based end user access to spam quarantines. This tool requires a database and a connection to an LDAP server to support user authentication.

Updated SPS

For users who have licensed Trend Micro Spam Prevention Solution (SPS), InterScan™ Messaging Security Suite incorporates an updated version of the SPS engine that provides more granular selection of spam filtering criteria. Using the updated SPS, administrators can configure spam detection based on an emphasis on catch rate or accuracy.

IntelliTrap

Trend Micro IntelliTrap is a new antivirus feature included in the InterScan™ Messaging Security Suite antivirus filter. Virus writers often attempt to circumvent virus filtering by using different file compression schemes. IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus compressed using these methods will enter your network via email.

Because there is the possibility that IntelliTrap may incorrectly identify a non-threat file as dangerous, Trend Micro recommends quarantining message attachments that fall into this category when the IntelliTrap feature is enabled. In addition, if your users regularly exchange compressed files, you may want to disable this feature.

This feature is turned on by default, and is configured to quarantine message attachments that fall into this category.

InterScan MSS main benefits

InterScan™ Messaging Security Suite includes the following benefits:

- Advanced Performance: InterScan MSS's enhanced virus/content scanner keeps your messaging system working at top performance. Its multi-threaded design takes full advantage of multi-processor systems.
- Domain-based Message Routing: You can flexibly configure email routing based on recipient domains.
- Integration with Trend Micro™ Control Manager™: As part of Outbreak Commander, the Trend Micro Control Manager™ delivers Outbreak Prevention Services. When TrendLabs detects a new email-borne virus, they issue a policy that uses the advanced content filters in InterScan MSS to block messages by identifying suspicious characteristics in these messages. These rules help minimize the window of opportunity for an infection before the updated pattern file is available.

Note: For additional information on Control Manager, see the *Trend Micro Control Manager Getting Started Guide*.

- POP3 Scanning: In addition to SMTP traffic, InterScan MSS can scan POP3 messages, at the gateway, as clients in your network retrieve them.

- Policy-based Management: You can define multiple virus and content filtering policies on a single InterScan MSS server to enforce your company's email usage guidelines. Define policies for individuals or groups, based on the sender and recipient addresses.
- Secure Web-based management console: Manage your InterScan MSS servers quickly and securely using an SSL-compatible, Web-based management console that provides access and session control.
- Integrated Messaging Content Filtering: A new and improved set of filters ensure email security by scanning message content and attachments.
- Mass Mailing Pattern: Mass mailing viruses are one of the biggest threats to a company's messaging system. Their speed of proliferation means that they can overwhelm mail servers within minutes of infection. InterScan MSS can automatically delete messages containing (or generated by) mass mailing viruses at the gateway. This helps prevent virus outbreaks in your network and minimizes any cleanup effort caused by the attack.
- Integrated Heuristic Spam Filtering: The Spam Prevention Solution (SPS) uses detection technology based on sophisticated content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high performance, real-time detection that is highly adaptable, even as spammers change their techniques.
- Administrator Quarantine Manager: Manage messages quarantined by the antivirus and content filters through the Web-based management console.
- Enhanced Server Access Control: Connection and relay restrictions prevent unauthorized use and relay from your InterScan MSS servers.
- System Availability Monitor: A built-in watchdog agent monitors the health of your InterScan MSS server and delivers notifications through email or SNMP trap when a fault condition threatens to disrupt the mail flow.

Understanding email policies

InterScan MSS uses rule-based policies to enforce your organization's email usage guidelines. You control the level of antivirus and content management applied to members of your organization. You can configure different policies for different people, based on job requirements or other business criteria.

A policy consists of the following attributes:

- Which messages the policy applies to
- What message or attachment characteristics are filtered, such as viruses, keyword expressions, or file types
- What actions to apply to messages that trigger the filter(s)

Is internal email traffic scanned?

InterScan MSS is a gateway antivirus and content management product. As long as messages pass through InterScan MSS's server, they are scanned. Internal messages may (or may not) pass through InterScan MSS, depending on your messaging system's topology. For more comprehensive protection at the mail server level, Trend Micro offers ScanMail.

Organizations can protect their network and business integrity with different policies for their various employees. Targeted user- and group-specific policies simplify antivirus and content management configuration, making them easier to maintain.

How it works

When the InterScan MSS server receives a message, it analyses the sender and recipient addresses to determine which policies apply. The filters configured for the applicable policies are applied and trigger a filter result. For each filter result, a corresponding filter action that dictates how the message is processed. The available processing actions include deliver, delete, or quarantine.

For more information about how InterScan MSS applies policies to message traffic, see *How the policy manager works* starting on page 4-2.

Chapter 2

Installing InterScan™ MSS

This chapter explains InterScan MSS installation procedures and requirements, including:

- Choosing your installation server
- Installation options
- Upgrading from previous versions
- Minimum system requirements
- Installing InterScan MSS
- Installing the Network Reputation Service
- Opening the InterScan MSS console
- Configuring InterScan MSS after installation
- Encrypting console-server communication using SSL
- Upgrading from the evaluation period
- Migrating settings to a new server

Choosing your installation server

For optimal performance, install InterScan MSS on a dedicated server with a configuration similar to your existing SMTP server. Apart from meeting the system requirements (see *Recommended system requirements* starting on page 2-25) there are no other special requirements.

Note: InterScan MSS's mail processing uses a store-and-forward mechanism, so a large capacity hard disk drive may be required, depending on the expected mail volume.

Installation options

InterScan MSS is deployed into an existing messaging environment at the SMTP gateway. It provides full access control, which allows you to restrict unauthorized connections and relays. InterScan MSS's domain-based routing capability provides flexible message delivery.

Note: Trend Micro does not recommend running more than one instance of IMSS on a single server. If you choose to run more than one instance of the software on a single server, the Centralized Reporting and Web-based quarantine tools will not work.

Installing without a firewall

The following figure illustrates how to deploy InterScan MSS and Postfix when your network does not have a firewall:

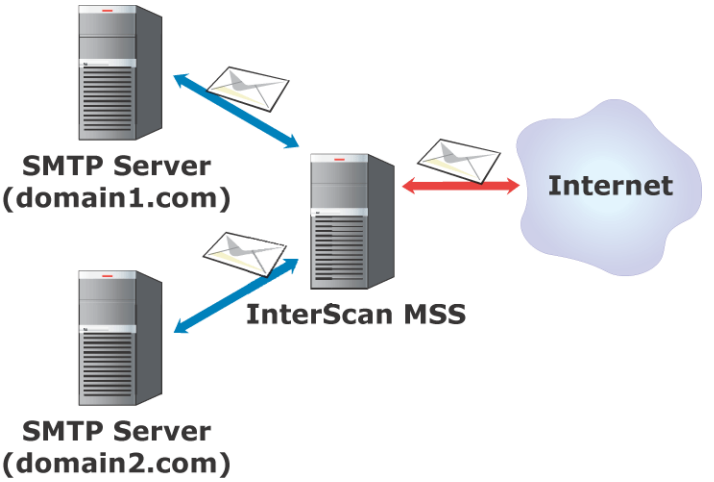


FIGURE 2-1. Installation topology: no firewall

Installing in front of the firewall

The following figure illustrates the installation topology when you install InterScan MSS in front of your firewall:

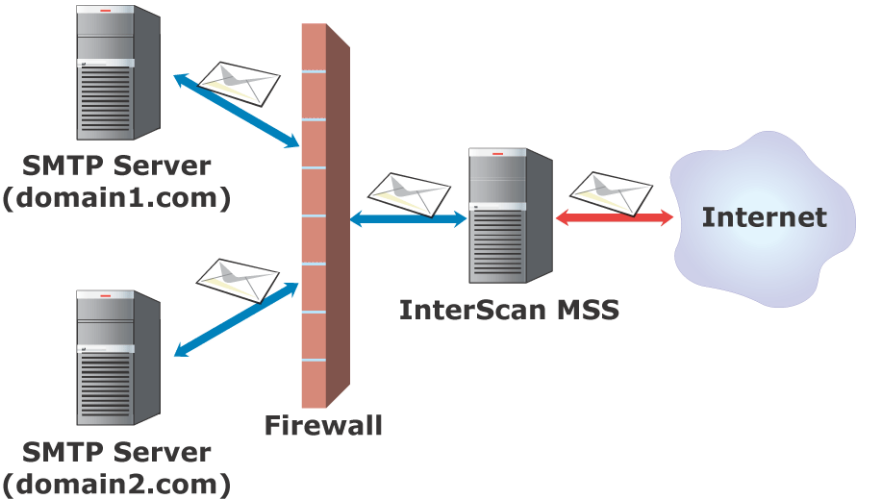


FIGURE 2-2. Installation topology: in front of the firewall

Incoming traffic

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

Outgoing traffic

- If there is no firewall, configure SMTP servers to route all outgoing email to Postfix and out to the Internet.
- If there is a firewall, configure the firewall (proxy-based) to route all outbound messages to InterScan MSS, so that:
  - Outgoing SMTP email goes to Postfix first and then InterScan™ MSS.
  - Incoming SMTP email can only come from Postfix to InterScan™ MSS.

- Configure InterScan MSS to allow internal SMTP gateways to relay, through Postfix, to any domain.

Installing behind a firewall

The following figure illustrates how to deploy InterScan MSS and Postfix behind your firewall:

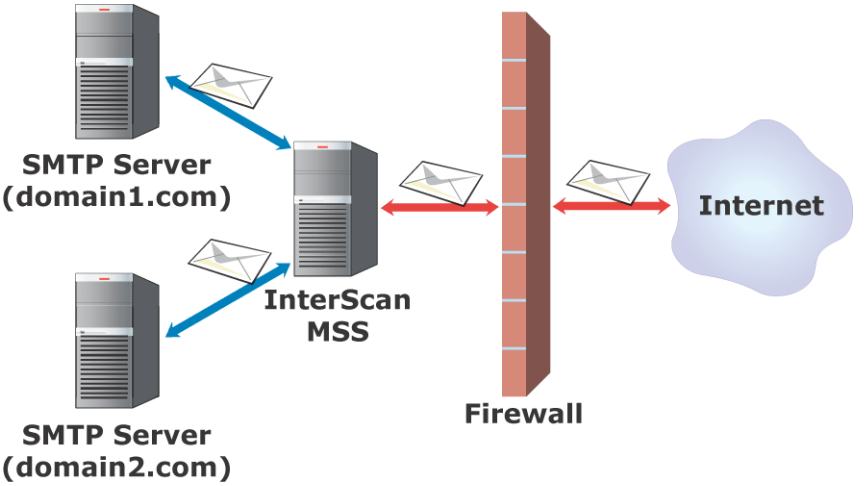


FIGURE 2-3. Installation scenario: behind a firewall

Incoming traffic

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

Outgoing traffic

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

Installing on a former SMTP gateway

The following figure illustrates how to install InterScan MSS and Postfix on the same server that formerly hosted your SMTP gateway:

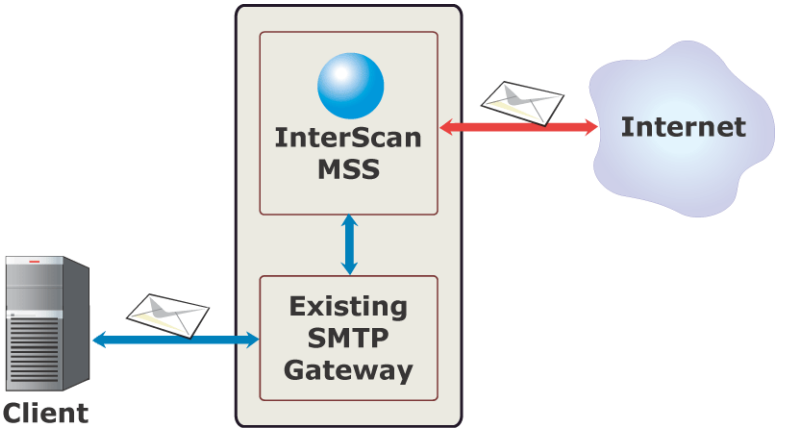


FIGURE 2-4. Installation scenario: on a former SMTP gateway

On the SMTP gateway:

- Allocate a new TCP/IP port to route SMTP mail to InterScan MSS. It must be a port not in use by any other service.
- Configure InterScan MSS to bind to the newly allocated port, which frees port 25.
- The existing SMTP gateway binds to port 25.

Incoming traffic

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

Outgoing traffic

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

In the DMZ

The following figure shows how to install InterScan MSS and Postfix in the DMZ:

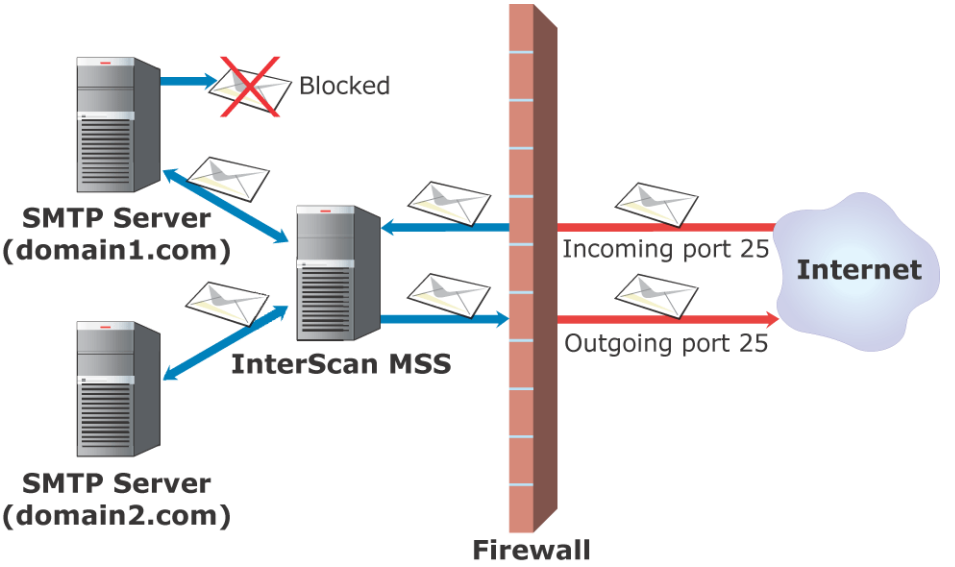


FIGURE 2-5. Installation scenario: in the DMZ

Incoming traffic

- Configure your proxy-based firewall, so that incoming and outgoing SMTP email can only go from the DMZ to the internal email servers.
- Configure your packet-based firewall.
- Configure Postfix and InterScan MSS to route email destined to your local domain(s) to the SMTP gateway or your internal mail server.

Outgoing traffic

- Configure Postfix to route all outgoing email (destined to other than the local domains) to the firewall or deliver using InterScan MSS.

- Configure all internal SMTP gateways to forward outgoing mail to Postfix and then to InterScan MSS.
- Configure InterScan MSS to allow internal SMTP gateways to relay, through Postfix and InterScan MSS, to any domain.

Postfix and the InterScan MSS scanning daemon

One Postfix instance as the MTA and one InterScan MSS daemon running on the same server:

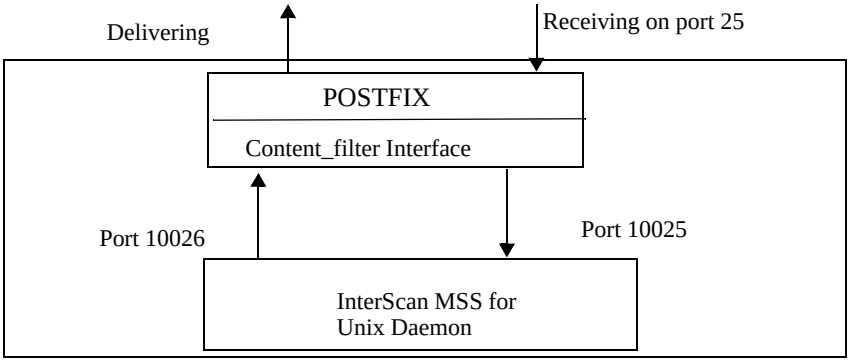


FIGURE 2-6. Postfix-InterScan MSS daemon configuration

This setup meets most of the needs of a small to medium-sized company and has low impact on the network since all the processes are running on the same server. Since they are sharing the same resources, however, this configuration requires a powerful server to host Postfix and the InterScan MSS daemon. See *Recommended system requirements* starting on page 2-25

Note: For more information about Unix daemons, see *InterScan™ Messaging Security Suite Daemons* starting on page A-11.

The default configuration parameters for both sides are:

In /etc/postfix/main.cf:

```
#IMSS:increase process limit from 50
default_process_limit=200


#IMSS:timeout parameters
imss_timeout=10m
imss_connect_timeout=1s


#IMSS:content filter interface thru transport “imss”
content_filter=imss:localhost:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=20
```

In /etc/postfix/master.cf:

```
#IMSS:content filter smtp transport “imss” for IMSS
imss unix - - n - - smtp
disable_dns_lookups=yes
smtp_connect_timeout=$imss_connect_timeout
smtp_data_done_timeout=$imss_timeout

#IMSS:content filter loop back smtpd
localhost:10026 inet n - n - 20 smtpd
content_filter=
smtpd_timeout=$imss_timeout
local_recipient_maps=
myhostname=localhost.$mydomain
smtpd_client_restrictions=
```

The “sandwich” configuration

In this configuration, one server hosts a Postfix instance as an upstream MTA for receiving and a second server hosts a Postfix instance as the downstream MTA for delivering. A third server hosts the InterScan MSS daemon, which sits between the two Postfix servers as a scanning proxy.

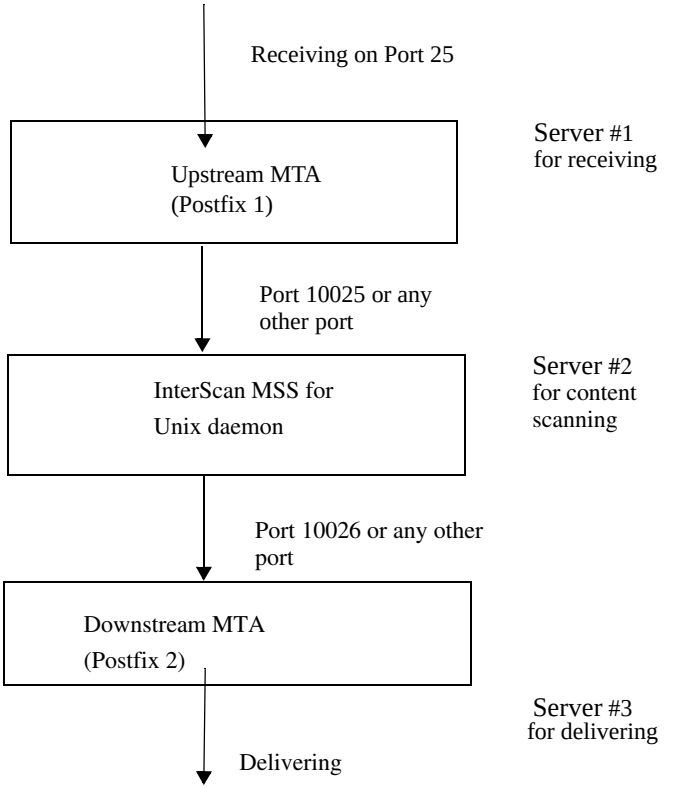


FIGURE 2-7. Sandwich configuration

This configuration is suitable for large corporations with heavy SMTP traffic. Each server has its own specific purpose and task and will not affect other servers. But, by using this type of setup, your network load will increase.

This configuration is highly flexible; you can replace Postfix with any SMTP MTA. But you are responsible for setting up connection control and domain relaying.

Here are the configuration settings if you use Postfix as the MTA:

- In /etc/postfix/main.cf on server#1, add the following to relay mail to server #2:

```
relayhost=smtp:[ip_of_server2]:10025
default_destination_recipient_limit=100
default_destination_concurrency_limit=50
```

- In /opt/trend/imss/config/imss.ini, open connection restrictions and point the downstream server IP to server#3:

```
imss socket binding address
[socket]
proxy_smtp_server_ip=all
[smtp]
smtp_allow_client_ip=127.0.0.1, ip_of_server1
downstream_smtp_server_addr=ip_of_server3
```

- In /etc/postfix/master.cf on server #3, modify smtpd settings to receive mail on port 10026:

```
10026 inet n - n - - smtpd
```

Configuring Postfix on a perimeter gateway

This section describes how to configure a Postfix perimeter gateway to relay incoming mail using SMTP to the mail hubs that ultimately host user mailboxes. The primary goal is to prevent Denial of Service (DoS) of incoming messages caused by a high volume of deferred outgoing messages. A secondary goal is to improve performance and lower the latency of incoming messages.

Tip: For a high volume mail server, Trend Micro recommends that you have a separate relay transport for incoming messages, as shown in the configuration below.

To configure Postfix:

1. In the `/etc/postfix/main.cf` file, add the following:

   #IMSS: relay transport for parallel delivery to the same domain or user relay

   smtp_connect_timeout=$relay_connect_timeout

2. In the `/etc/postfix/main.cf` file, add the following:

   `#IMSS:` connection timeout for relay transport

Note: If multiple MX hosts are available, set relay_connect_timeout=1s

relay_connect_timeout=30s

#IMSS: “relay” transport rate control.

Note: You can raise these two limits depending on your environment, such as the downstream MTA's capacity, or the number of perimeter hosts.

relay_destination_recipient_limit=50

relay_destination_concurrency_limit=50

Depending on your lookup table file type, set:

transport_maps = dbm:$config_directory/transport

3. In the `/etc/postfix/transport` directory path, add your destination domain name and the hostname of the next hop with “relay” transport:

Note: If MX records are not used, set the entry to relay:[nexthop] to suppress MX lookups on the nexthop hostname.

```
your.domain.name relay:next hop
```

4. Rebuild the transport lookup table and reload Postfix.

```
#postmap /etc/postfix/transport
#postifx reload
```

Multiple daemons on the same server

This section describes how to configure multiple InterScan MSS scan services on the same server.

By default, InterScan MSS is configured to run only one instance on a given server. However, if you want to run two instances of InterScan MSS on one server, for example, one for incoming messages, the other for outgoing messages with different policy settings, you can do so with this information.

To set up multiple InterScan MSS daemons:

1. Copy the InterScan MSS system-installed directories (for example, /opt/trend/imss) and, for process tracking purposes, change the name of the two binaries (regserver and imssd) in the new directory.
2. Do the following:
   a. # cp -rp /opt/trend/imss /opt/trend/imss2
   b. # cd /opt/trend/imss2/bin
   c. # mv regserver regserver2
   d. # mv imssd imssd2
3. Open the script file /opt/trend/imss2/script/S99Reg and do the following:
   a. Change the line IMSS_HOME=/opt/trend/imss to IMSS_HOME=/opt/trend/imss2.

b. Find all instances of “regserver” and change them to “regserver2”.

4. Open the script file /opt/trend/imss2/script/S99IMSS and do the following:

a. Change the line IMSS_HOME=/opt/trend/imss to IMSS_HOME=/opt/trend/imss2.

b. Find all instances of “imssd” and change them to “imssd2”.

5. Open the config file /opt/trend/imss2/config/imss.ini and do the following:

a. Find all instances of “/opt/trend/imss” and change them to “/opt/trend/imss2”.

b. Change the following parameters:

[EMANAGER_REGSERVER] EMANAGER_REGSERVER_PORT=5060 to EMANAGER_REGSERVER_PORT=5061 (or any available port number).

[smtp]

downstream_smtp_server_addr=127.0.0.1

downstream_smtp_server_port=10026 to downstream_smtp_server_addr=xxxxxxxxx

downstream_smtp_server_port=xxxxxxxxx

Note: The IP/port of the downstream MTA handles requests from this particular InterScan MSS scanning daemon. It is usually the second instance of Postfix that is running on the localhost.

[socket_1]

proxy_service =SMTP_SERVICE
proxy_port=10025

to

proxy_service=SMTP_SERVICE
proxy_port=10125 (or any available port number)

Note: After you change this parameter, modify the relay port number of the upstream MTA that forwards requests to this particular InterScan MSS scanning instance. For example, in /etc/postfix/main.cf: content_filter = smtp:localhost:10025.

---

c. In the [socket_2] section, change: proxy_service=POP3_GENERIC_SERVICE proxy_port=110 to proxy_service=POP3_GENERIC_SERVICE proxy_port=11000 (or any available port number).

Note: If you do not need POP3 service for the second instance of InterScan MSS daemon, turn it off by changing the following parameters: in the [pop3] section, change pop3__enable_proxy=yes to pop3_enable_proxy=no.

---

d. In the [General-Notification] section, change: NotificationSMTPAddr=127.0.0.1:10026 to NotificationSMTPAddr=xxxxxxx:xxxxx

---

Note: The MTA's IP/port number is responsible for notification email delivery. This value is usually the downstream MTA that handles requests for this particular instance of the InterScan MSS daemon.

---

6. Replace /opt/trend/imss2/config/eMan_db.xml file with policies that are different from the first instance.
7. Start the second registry server (# **`/opt/trend/imss2/script/S99Reg start`**)
8. Start the second InterScan MSS daemon service (# **`opt/trend/imss2/script/S99IMSS start`**)

Sendmail daemons and InterScan MSS

The following illustration depicts running two Sendmail daemons and InterScan MSS on the same Unix server.

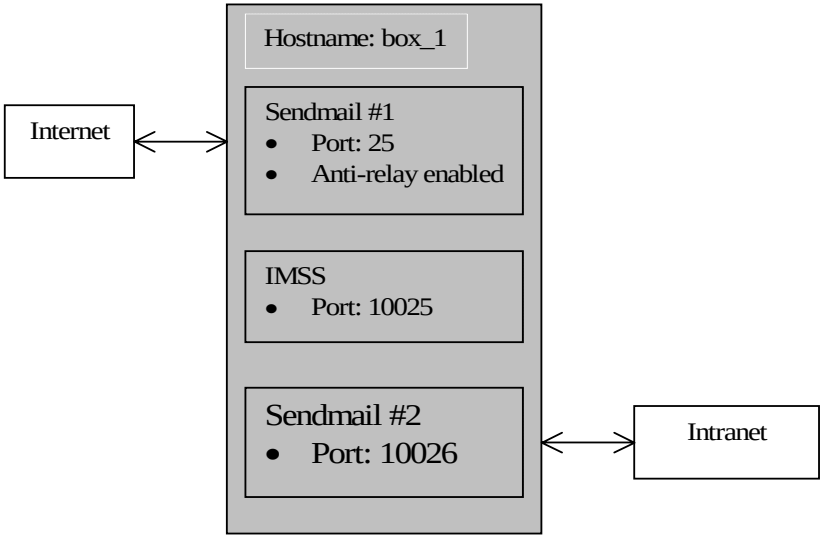


FIGURE 2-8. Sendmail daemons and InterScan MSS on one server

Port 10025 and 10026 are arbitrary port numbers, so replace 10025 and 10026 with free ports when completing the configuration below. (Port 25 is the standard SMTP port.)

The instructions to configure Sendmail daemons for this configuration are:

Configure Sendmail #1

To configure Sendmail #1:

1. Copy the Sendmail.cf file called Sendmail.cf.delivery.
2. Change the A option in sendmail.cf for Msmtp, Mesmtp, Msmtp8, and Mrelay from “IPC $h” to “IPC localhost 10025”, where 10025 is an arbitrary free port on box_1.
3. Add the “k” flag to the “F” option for Msmtp, Mesmtp, Msmtp8, and Mrelay in sendmail.cf.

   The changes for Msmtp (as an example) should look as follows:

   Msmtp Before:

   P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990,

   T=DNS/RFC822/SMTP,

   A=IPC $h

   Msmtp After:

   P=[IPC], F=kmDFMuX, S=11/31, R=21, E=\r\n, L=990,

   T=DNS/RFC822/SMTP,

   A=IPC localhost 10025
4. Replace the local mailer with [IPC] for Mlocal in sendmail.cf.
5. Change the A option to “IPC localhost 10025” for Mlocal in sendmail.cf.
6. Add the “k” flag to the “F” option for Mlocal in sendmail.cf.
   The changes for Mlocal look as follows:

   Mlocal Before:

   P=/usr/lib/mail.local, F=lsDFMAw5:/|@qfSmn9, S=10/30, R=20/40,

   T=DNS/RFC822/X-Unix,

   A=mail.local -d $u

Mlocal After:

P=[IPC], F=klsDFMAw5:/|@qSmn9, S=10/30, R=20/40,

T=DNS/RFC822/X-Unix,

A=IPC localhost 10025

Note: Make sure the "F" option of Mlocal does not include the "f'" flag. This flag is standard on the Solaris 7 distribution of Sendmail and you should remove it.

Configure Sendmail #2

To configure Sendmail #2:

1. Change the listening port to 10026 in sendmail.cf.delivery file.
   Before:

   #O DaemonPortOptions=Port=esmtp

   After:

   O DaemonPortOptions=Port=10026

2. Change the mail queue to a different directory in sendmail.cf.delivery.
   Before:

   O QueueDirectory=/var/spool/mqueue

   After:

   O QueueDirectory=/var/spool/mqueue1

3. Create the directory /var/spool/mqueue1 and make sure it has the same ownership and permissions as the original in /var/spool/mqueue.
4. Add the "k" flag to the F option for Mlocal, Msmtp, Mesmtp, Msmtp8, and Mrelay in sendmail.cf.delivery.

Restarting Sendmail services

To finish sendmail setup, restart Sendmail services:

5. Restart the first Sendmail daemon to receive SMTP traffic on port 25 using the following command:

   ```
   /usr/lib/sendmail –bd –q1h
   ```

6. Restart the second Sendmail daemon to receive SMTP traffic from InterScan MSS using the following command:

   ```
   /usr/lib/sendmail –bd –q1h –C/etc/mail/sendmail.cf.delivery
   ```

Special information about Web End-user Quarantine (EUQ) and Network Reputation Service (NRS)

If you will be deploying the Trend Micro Network Reputation Service IP filter or the Web End-user Quarantine tools, there are some additional network topology considerations you must address.

Deploying InterScan MSS with IP Filtering

The Trend Micro Network Reputation Service uses IP filtering to block connections at the IP level. Based on information gather through the Trend Micro Threat Reputation Network, the NRS filter determines if the computer initiating an SMTP connection is a known sender of spam. Because the connecting computer's IP address must be accessible to Network Reputation Service, no address modification can occur between the edge of your network and the connection to Network Reputation Service.

Note: This means that any firewall between Network Reputation Service and the edge of your network must be of a type that does not modify the connecting IP address, or must be configured not to do so.

If IMSS always accepts SMTP connections from a router, for instance, the IP filter will not work, as this address would be the same for every received message and the IP filtering software would be unable to determine if the original initiator of the SMTP session was a known sender of spam.

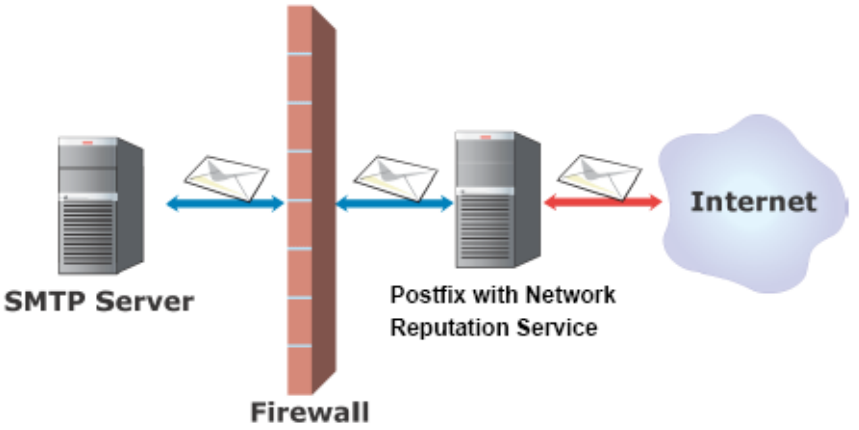


FIGURE 2-9. Installation of IMSS configured for the Trend Micro Network Reputation Service

Deploying InterScan MSS with Web-based EUQ

The Trend Micro Web-based EUQ tool allows you to provide end users access to messages which IMSS has quarantined as spam. It is possible to deploy the Web-based EUQ tool on the same server as InterScan™ Messaging Security Suite, or on a separate server.

For the end users in your organization to be able to access the Web-based quarantine, they must have HTTP access to the server. In addition, server hosting the EUQ tool must be able to connect to the database that IMSS uses to store information about quarantined items.

Note: This means that any firewall between EUQ and end-user computers on your network must be of a type that does not prevent HTTP connections from internal addresses, or must be configured to allow such traffic.

Deploying InterScan MSS with Web-based EUQ on a single server

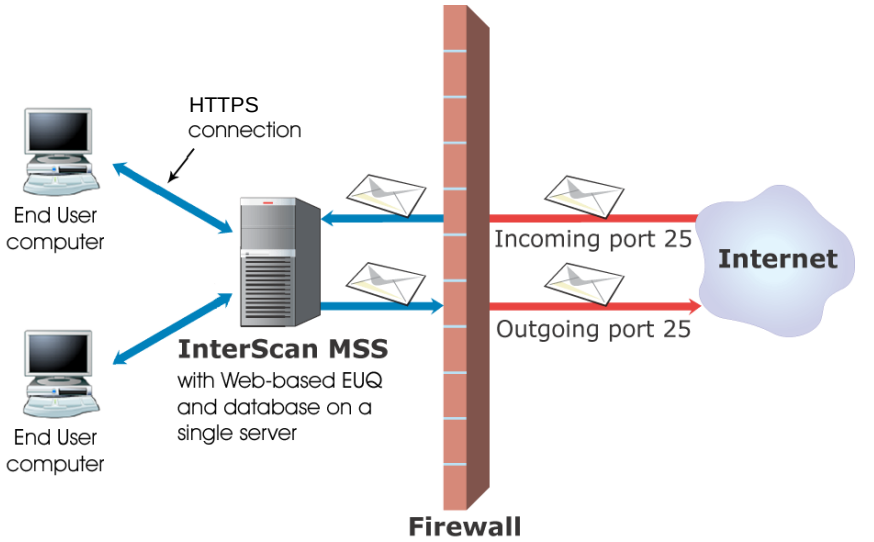


FIGURE 2-10. Installation of IMSS, Web-based EUQ, and database on a single server

Deploying InterScan MSS and Web-based EUQ on separate servers

You can also install Web-based quarantine and the database on a separate server from IMSS. In this case, you must configure any firewall between IMSS and the other server to allow database connections between them.

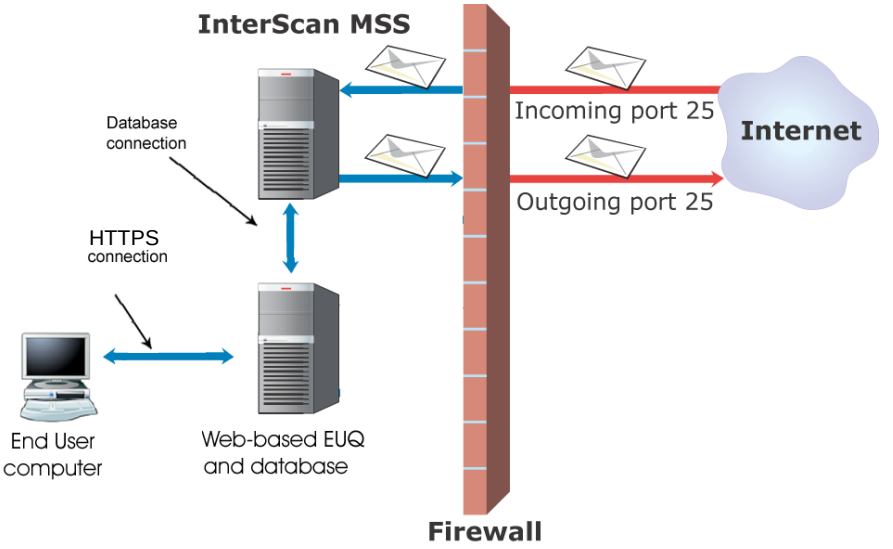


FIGURE 2-11. Installation of IMSS on one server and Web-based EUQ and database on a separate server

---

Note: You can only install one instance of Web End-user Quarantine (EUQ) per group of IMSS servers.

Communication Between Servers

If you have an internal firewall, it must be configured to allow communication between IMSS, the EUQ Server, and the database. For instance, if you install the EUQ server on one system, and the database on another, you must configure any firewall between the two systems to allow communication on port 5432, which is the port that they use for database connectivity.

Upgrading from previous versions

The InterScan™ Messaging Security Suite installation program can automatically upgrade from version 5.5 of InterScan MSS on the supported platforms. If the installation program detects this version, it can:

- Uninstall the previous version of InterScan MSS
- Install InterScan MSS
- Migrate the existing settings

Note: If you choose not to migrate your old InterScan MSS settings, we recommend that you completely uninstall InterScan MSS and then do a clean install, rather than installing InterScan MSS 5.7 over an existing installation.

The installation program saves the settings from your previous installation, so if your license is still valid, you do not need to make any changes. If your previous license has expired, once you have completed migration, you will need to activate Trend Micro Antivirus and eManager. For more information on activating InterScan MSS, see *Activating Trend Micro Antivirus and eManager, and the Spam Prevention Solution (SPS)* starting on page 2-40.

Recommended system requirements

The following table provides recommended and minimum system requirements for running InterScan™ Messaging Security Suite.

	Solaris	Linux
	Sun™ Solaris™ 2.8 or 2.9	Red Hat Enterprise Linux version 2.1 or 3 SuSE(TM) Linux Enterprise Server version 8.0 or 9.0
Recommended	UltraSPARC™ III processor 1GHz	Intel Pentium® III 1GHz or above
Minimum	UltraSPARC™ II processor 650MHz	Intel Pentium® III 650MHz CPU
Recommended	2GB RAM	
Minimum	1GB RAM	
Recommended	2GB disk space for mail storage	
Minimum	1GB disk space for mail storage	
Recommended	4GB swap space	
Minimum	2GB swap space	
System Kernel	In etc/system set semsys:seminfo_semmni=315 set semsys:seminfo_semmsl=300 set semsys:seminfo_semmns=630 set semsys:seminfo_semopm=315 set semsys: seminfo_semvmx=32767 set shmsys: shminfo_shmmax=4294967295 set shmsys:shminfo_shmmni=315 set shmsys:shminfo_shmseg=10 set shmsys:shminfo_shmmin=1	

If you are installing either the Centralized Reporting or Web-based End User Quarantine tool, you must install a supported version of the PostgreSQL database software. InterScan™ Messaging Security Suite currently supports PostgreSQL version 7.4.8 or above.

Note: To correctly display error messages, you must install and enable Java for your Web browser. This requirement applies to both the Internet Explorer and Mozilla browsers.

Installing InterScan Messaging Security Suite

To install InterScan MSS:

Note: The information in Step 1 applies **only** to Solaris.

Before installing InterScan MSS:

1. Install the following Solaris patches in this order:
   - 108714
   - 108652
   - 108773
   - 108921
   - 112003
   - 111293
   - 112396
   - 108987
   - 111111
   - 111310
   - 108528
   - 108827
   - 108940
   - 112472
   - 108434 (32-Bit Shared library patch for C++)
   - 108435 (64-Bit Shared library patch for C++)
   - 107311

2. Run ./postfixinstall.sh postfix.

   If you install Sendmail on the same Linux server as Postfix, first manually stop Sendmail and then open Postfix.

Note: Trend Micro strongly recommends that you install and use the Postfix distributed with your distribution of Linux (Red Hat® or SuSE Linux).

3. If Postfix is not bundled in the InterScan MSS package, configure the Postfix settings to work with InterScan MSS by changing the following values:

   In postfix configuration file main.cf:

```
#IMSS: increase process limit from 50
default_process_limit=200
imss_timeout=10m
imss_connect_timeout=1s
#IMSS: content filter interface thru transport “imss”
content_filter = imss:localhost:10025
imss_destination_recipient_limit=200
imss_destination_concurrency_limit=20
```

In postfix configuration file master.cf:

```
#IMSS: content filter smtp transport “imss” for IMSS
imss      unix  -   -   n   -   -   smtp
        -o disable_dns_lookups=yes
        -o smtp_connect_timeout=$imss_connect_timeout
        -o smtp_data_done_timeout=$imss_timeout

#IMSS: content filter loop back smtpd
localhost:10026 inet n - n - 20 smtpd
       -o content_filter=
       -o smtpd_timeout=$imss_timeout
       -o local_recipient_maps=
       -o myhostname=localhost.$mydomain
       -o smtpd_client_restrictions=
```

4. When you have completed the installation and configured InterScan™ Messaging Security Suite, enable message traffic by editing the `imss.ini` file. Under the `[smtp]` section, change the `smtp_enable_proxy` parameter to `smtp_enable_proxy=yes`

Understanding installation methods

There are two ways to install InterScan MSS:

- Interactive, which prompts you for input during the installation
- Silent, which gets installation parameters from a predefined file

Using interactive installation

If you decide to install the Control Manager agent, install the Control Manager server first and then get the account and IP or hostname information (for additional information, see *Opening the IMSS management console* starting on page 2-38).

The following is a list of the key steps during an interactive installation:

1. Log in as a superuser and go the installation package directory.
2. Type `./isinst`.
3. Follow the prompts to install InterScan MSS. You will be asked to specify:
   - The installation path
   - The License Agreement
   - The mail server domain name
   - Whether you want to enable IntelliTrap
   - Whether you want detected attachments sent to TrendLabs for analysis
   - Whether you want to install the InterScan MSS Web console
   - Whether you want to configure Postfix through the Web console
   - Whether to install the Trend Micro Control Manager agent
   - Whether you want to install AMON
   - Whether to install the IMSS Perl report tool
   - Whether to install the Centralized Spam Reporting and EUQ
   - Whether to install a PostgreSQL database or point to an existing database
   - Your Activation Code
   - Proxy settings to connect to the Internet
4. Ensure that the memory or swap space is adequate (for additional information, See *Recommended system requirements* on page 2-25).
5. When prompted to install the Control Manager agent, enter **y** or **n**.

Using silent installation

For a silent installation, configure the parameters (listed below) in the `isinst.ini` file with the appropriate information. When you correctly configure this .ini file, the installation process proceeds without prompting you for responses.

The configuration parameters are:

Configuration Parameter	Description
installAmon=no	This parameter determines if the AMON tools will be installed.
AutoRegistAV=no	This parameter determines if Antivirus and eManager will be registered during installation. The choices are yes or no. The default is no.
AutoRegistSPS=no	This parameter determines if SPS will be registered during installation. The choices are yes or no. The default is no.
AVActivateCode=	This is your Antivirus and eManager Activation Code. The default is null.
ProxyIP=	Specifies the IP address of your proxy server.
ProxyPassword=	Specifies the password to use when accessing your proxy server.
ProxyPort=	Specifies the port to use when accessing your proxy server.
ProxyUser=	Specifies the user name to use when accessing your proxy server.
UseProxy=	This parameter specifies whether your server uses a proxy to access the Internet. The default is no.
UseSock4Proxy=no	This parameter specifies whether your proxy is a SOCKS4 proxy. The default is no.
AgentEntityname=	This parameter suppiles hostname of the server where IMSS is installed in the Control Manager interface.

Configuration Parameter	Description
AJP12PORTNUM=8007	If this port conflicts, the CCGI install will fail.
AJP13PORTNUM=8009	If this port conflicts, the CCGI install will fail.
ByPassPostfixPages=	Assuming you are using the Web administrative interface, this parameter allows you to manage a subset of Postfix configurations through the Web interface.
ByPassUI=	This parameter allows you to skip installation of the Web administrative interface component. When the value is “No”, the installation program installs the Web UI. If the value is “Yes”, the installation program does not install the Web UI.
cmserveraccount=	This parameter is for the Control Manager server account information.
cmserverip=	This parameter is for the Control Manager server IP address.
dbpass=	This parameter specifies the password for the user when connecting to the database.
dbuser=	This parameter specifies the user name when connecting to the database.
enableForward=	If set to "Yes," samples of detected threats are sent to TrendLabs. The default is "No."
enableIntelliTrap=	If set to "Yes" (which is the default), IntelliTrap is enabled.
EUQPORTNUM=8446	If this port conflicts, the EUQ or central report install will fail.
EUQPORTNUM=8447	If this port conflicts, the EUQ or central report install will fail.
existImssaction=migration	When a previous version of IMSS is installed, this parameter controls whether the installation program will remove the older version or stop. The choices are: migration, remove or exit. To uninstall the old version, set the parameter to `remove` To migrate, set the parameter to `migration`.

Configuration Parameter	Description
HTTPPORTNUM=8081	If this port conflicts, the CCGI install will fail.
HTTPSPORTNUM=8445	If this port conflicts, the CCGI install will fail.
install_path=	This is the installation path, and the default value is /opt/trend.
InstallAgent=	This parameter allows you to begin the Control Manager agent installation process. The default value is no.
installCreport=	Install the Centralized Reporting software
installDB=	Specifies whether to Install the PostgreSQL database software. If no, you must configure dbuser, dbpass, and sqlserver.
installPreport=	Install the Perl Reporting package
mailserverdomain=	You must specify a domain name, or the silent installation will stop.
SPSActivateCode=	This is your SPS Activation Code. The default is null.
sqlserver=	Specifies the IP of the database server where PostgreSQL is running.
UseExistingIMSSTable=	Choices are "Yes" or "No" to specify whether to use existing IMSS tables in the running database.

Table 2-1. Configuration Parameters and Their Descriptions

Note: The relationship between settings “UseProxy” and “UseSock4Proxy”:

Use Proxy Setting	UseSock4Proxy Setting	Outcome
No	N/A	No proxy will be used
Yes	No	The proxy settings use the values from the ProxyIP, ProxyPort, ProxyUser, and ProxyPassword parameters
Yes	Yes	Use SOCKS4 Proxy

Default sub-policy domain information

For a silent or an interactive installation, submit a valid mail server domain name for your organization.

Note: A valid mail server domain is extremely important when defining incoming or outgoing policies for InterScan MSS server mail traffic.

During an interactive installation, InterScan MSS uses the mail server's domain information that you provided and writes this information to the default sub-policies (for more information on sub-policies, *Creating sub-policies* starting on page 4-21).

During a silent installation, before you begin, ensure that you have correctly configured the `mailserverdomain` value. If this value is null, the script will stop the installation and prompt you to configure a mail server domain and re-install InterScan MSS.

Verifying the installation

After the installation is complete, to see a list of the daemons, type the following at the command prompt:

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

Telnet to port 25 to ensure that InterScan MSS/Postfix answers.

Trend Micro Network Reputation Service (NRS)

The Trend Micro Network Reputation Service (licensed separately) provides spam filtering at the connection level. It identifies known spam senders by IP address and refuses SMTP connections from these senders. This significantly reduces the amount of traffic that the IMSS server must process against other rules.

Installing Trend Micro Network Reputation Service (NRS)

The Trend Micro Network Reputation Service runs on a modified Postfix installation. The NRS installation script modifies the Postfix configuration files and installs a log parser to allow IP filter reporting. During installation, you will also be asked for an NRS Activation Code and for information about your IMSS Centralized Reporting database. You should install the database before installing the Network Reputation Service. If you do not require Centralized Reporting, you can choose not to install it during the installation process.

Note: The Network Reputation Service utilizes Perl's DBI for database connectivity, so no ODBC driver is required. However, you must install the Perl DBI module and Pg DBD (PostgreSQL DB driver) before installing the NRS log parser for reporting.

To install Network Reputation Service:

1. Log on to the server where NRS will run.

   Note: Note: This server must already have an instance of Postfix installed. It must also be able to connect to the Centralized Reporting database and the server that is processing your messaging (most likely the IMSS server). Trend Micro does not recommend running NRS on the same server as InterScan™ Messaging Security Suite or the IMSS Centralized Reporting database.

   ---

2. Unzip and then unTar the installation package.
3. Run the install script install.sh

4. Follow the prompts to configure NRS:
   a. Type your Activation Code.

   Note: When typing your Activation Code, omit the hyphens and type only the characters and numbers.

   b. Type the database IP address.
   c. Type the database name.
   d. Type the user name and password that NRS will use to access the database.
   e. Once the install is complete, Postfix will restart and the NRS service will be active.

Understanding centralized spam reporting and end-user quarantine (EUQ)

InterScan MSS provides a new centralized spam reporting function and Web-based EUQ to improve spam management. The centralized spam reporting tool can aggregate spam data from multiple InterScan™ Messaging Security Suite servers and provide reports that reflect the total volume of spam processed across all servers. This allows administrators to obtain a more complete picture of how spam is affecting their network.

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

Both of these components require a PostgreSQL database for data storage.

Note: Only one instance of the Centralized Reporting and EUQ Admin console component can be installed per database.

Opening the IMSS management console

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

To view the console in a browser, go to:

- http://<Imss_server (or IP):8081>/IMSS.html
- https://<Imss_server (or IP):8445>/IMSS.html

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

The default password for the InterScan MSS console is "imss" in lowercase, without the quotes. Type the password into the password field the first time you open the console and click the **Enter** button. To prevent unauthorized changes to your policies, we recommend that you configure a password immediately following installation. See *Setting the InterScan MSS password* starting on page 3-26 for more information.

Viewing the management console using SSL

The InterScan MSS management console supports encrypted communication, using SSL. After installing the InterScan MSS, 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, run the following:

```
$IMSS_HOME/apache/bin/mkcert.sh
```

Opening the centralized spam reporting and EUQ console

The centralized spam reporting and EUQ management console can be viewed with a Web browser from the machine where the program was installed or remotely across the network.

To view the console from another computer on the network, go to:

```
https://<target server's IP address>:8447
```

For example, `https://127.0.0.0:8447`

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

The password for the InterScan MSS centralized spam reporting and EUQ console is "imss" in lower case, without the quotes. To prevent unauthorized changes to your policies, Trend Micro recommends changing the password regularly.

If InterScan MSS is installed on a multi-homed machine with multiple IP addresses, use the IP or FQDN of the Default Web Server in IIS.

Configuring InterScan MSS after installation

Once you have finished installing the software, perform the following configuration tasks using the InterScan MSS management console.

Activating Trend Micro Antivirus and eManager, and the Spam Prevention Solution (SPS)

When the InterScan Messaging Security Suite Web console starts for the first time, it opens directly to the product activation page.

WARNING! Until you activate the InterScan MSS components, the system does not perform any scanning

In order to activate Trend Micro Antivirus and eManager, or the Spam Prevention Solution, you need to enter a valid Activation Code for each product. There are several ways to obtain an Activation Code:

- As part of the product download
- Through a reseller
- Directly from the Trend Micro Web site

To enter your Activation Code:

1. Go to the product license page by clicking **Configuration** > **Product Licenses**.
2. Click the product you want to activate.
3. Enter your Activation Code.
4. Click OK.
5. When you return to the **Product Licenses** page, the status of the product you activated will be **Active**.

Note: If you do not have an Activation Code, obtain one by registering your product online through the Trend Micro Web site. You will need to enter your Registration Key (if applicable) and email address, along with additional registration information. Once you have completed the product registration process, you will receive an Activation Code by email

Controlling message relay

The InterScan MSS server can relay messages to mail hosts in your intranet and to mail hosts on the Internet. The default relay configuration after an installation ensures that the program is not set up for "open relay."

This means that:

- Servers outside your intranet can only relay messages that are destined for the domain you provided during installation.
- Internal mail servers cannot relay messages to the Internet.

To change the default anti-relay settings, in the left frame, click **Configuration** > **Postfix** > **Receiver** > **Relay Control**. For more information, see *Relay control* starting on page 3-10.

Note: If you want InterScan MSS to protect multiple domains, add these additional domains to the **Allowed Relay Destinations** list.

Modifying the message routing table

The delivery method InterScan MSS uses after messages are processed is determined by the message routing table and the domain shown in the message's destination address. The InterScan MSS installation program creates a basic routing table based on the domain name destination of email messages. This table routes all messages destined for the domain using SmartHost (a way to route mail to separate destinations), depending on the delivery method you specified during installation. Messages destined to all other domains use Postfix to resolve the destination address.

To modify your **Postfix Domain-Based Delivery** settings, in the left frame, click **Configuration** > **Postfix** > **Domain-Based Delivery**.

To modify your **SMTP Routing Domain-Based Delivery** settings:

- In the navigation panel, click **Configuration** > **Postfix** > **Domain-Based Delivery**.

For more information see *Domain-based delivery* starting on page 3-12.

Updating InterScan MSS

Trend Micro frequently updates the virus pattern file (sometimes several times a week) in response to newly released viruses. Updates to the scan engine occur when needed to enhance its functionality and performance. In addition, Trend Micro updates the spam scanning rules used by the heuristic spam filter (SPS) when necessary to enhance its spam identification capabilities.

To update your software, in the navigation panel, click **Configuration** > **Update** > **Update Now**.

For more information about on-demand program updates, see *Using on-demand update (Update Now)* on page 3-23.

Configuring Scheduled Update

InterScan MSS can automatically check the Trend Micro update server at a user-configured interval.

To configure an update schedule, in the navigation panel, click **Configuration** > **Update** > **Scheduled Update**.

For more information, see *Scheduling updates* starting on page 3-23.

Note: If the InterScan MSS server connects to the Internet using a proxy server, enter the proxy settings before you attempt to update.

Upgrading from the evaluation period

If you entered an evaluation Activation Code for InterScan MSS or Spam Prevention Solution (SPS) when you activated the product, you started an evaluation period that allows you to try out the full functionality of the software. You can upgrade from the evaluation period to the registered version of either product at any time by entering valid Activation Codes in the Web console.

To enter Activation Codes:

1. Open the InterScan MSS Web console.
2. In the navigation panel, click **Configuration** >**Product Licenses**.
3. Click the product you want to activate.
4. Enter your Activation Code.
5. Click **OK**.

Backing up and replicating data

The information in this section allows you to perform a data backup and replication in a homogeneous environment (InterScan MSS instances of the same release, the same OS platform, and the same language).

WARNING! This process will **only** replicate configurations across InterScan MSS instances of the same release, the same OS platform, and the same language. If you attempt a data backup and replication across a heterogeneous environment, the target InterScan MSS installation will encounter unrecoverable system errors.

You can install InterScan MSS in any directory. However, to complete a replication with Trend Micro™ Control Manager™, you must install the software in the same directory on both the source and destination server (for example, /opt/trend). Since eMan_db.xml is a database file for eManager, to backup or replicate settings, copy imss.ini and eMan_db.xml.

The replication process replicates the policy database and the imss.ini file, but the target server's imss.ini retains the following server-specific settings:

For the policy database:

Spam database file path

```
<key keyName="f_vec_strSpamList">
<value type="sz"
valueName="sz_001">/opt/trend/imss/lib/TM_AntiSPam.56
8</value>
<value type="sz"
valueName="sz_002">/opt/trend/imss/lib/TM_Trend$SE.18
4</value>
```

For `imss.ini`:

Each server has its own IP address.

```
smtp_allow_client_ip=127.0.0.1, x.x.x.x
```

Each server has its own pattern file, scan engine, and spam database and their update dates.

```
[Update]
PatternVersion=
EngineVersion=
SPAMDBVersion=
UpdatePatternDate=
UpdateEngineDate=
UpdateSPAMDBDate=
```

Chapter 3

Configuring InterScan™ MSS

This chapter explains important post-installation configuration tasks to perform. Topics include how to customize your InterScan MSS configuration settings and how to perform routine administrative tasks to keep your software up-to-date.

The following topics are covered:

- Working with the InterScan MSS console
- Configuring services
- Configuring the Postfix settings
- Scanning POP3 messages
- Configuring email clients
- Changing InterScan MSS's message processing directories
- Updating your virus pattern, scan engine, and spam database
- Viewing and maintaining log files
- Changing the management console password
- Registering your software
- Updating an evaluation version to the full version
- Modifying the XML configuration file

Opening the InterScan MSS console

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

To view the console in a browser, go to:

- http://<Imss_server (or IP):8081>/IMSS.html
- https://<Imss_server (or IP):8445>/IMSS.html

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

The default password for the InterScan MSS console is "imss" in lowercase, without the quotes. Type the password into the password field the first time you open the console and click the **Enter** button. To prevent unauthorized changes to your policies, we recommend that you configure a password immediately following installation. See *Setting the InterScan MSS password* starting on page 3-26 for more information.

Using online help

The InterScan MSS Web console includes page-specific online help that you can view from most of the console's pages. To view context-sensitive help topics, click the help icon that appears in the top-right corner of most screens. To view the online help system's table of contents, click **Help** at the bottom of each page.

If, after checking the program documentation, you still have questions, see *Troubleshooting and Contact Information* starting on page 9-1 for additional information about accessing technical support, such as self-service support through the Trend Micro on-line Knowledge Base. For more information, see the section on the Trend Micro *Knowledge Base* starting on page 9-7

Applying configuration changes

InterScan MSS saves configuration settings in both an XML file and an .ini file on the server. For maximum efficiency, InterScan MSS writes a copy of this data into memory when the service starts to improve program performance. For the program to use the new configuration settings, InterScan MSS needs to read the updated settings from the XML or.ini file and apply them.

When you click **Apply Now**, InterScan MSS reads the new data from the configuration files and applies the changes. To apply other configuration changes, such as changing the directories used for message processing or changing the mail settings, you must restart the InterScan MSS service.

When you make configuration changes in the InterScan MSS console, they are processed in one of these two ways:

Settings applied automatically after saving

InterScan™ Messaging Security Suite applies these configuration changes automatically after they are set in the console:

- Changes to the InterScan MSS console password. For more information, see *Setting the InterScan MSS password* starting on page 3-26

- Scan engine, virus pattern, and spam pattern and anti-spam engine **Update Now** settings. For more information, see *Using on-demand update (Update Now)* starting on page 3-23
- Proxy server settings. For more information, see *Configuring proxy settings* starting on page 3-22
- Scan engine, virus pattern, and spam pattern and anti-spam engine **Scheduled Update** settings. For more information, see *Scheduling updates* starting on page 3-23

Note: InterScan MSS also automatically applies all update-related settings, including proxy server information, to the InterScan MSS Scheduler program.

- All virus, eManager and **Program Log** viewing settings. For more information, see *Working with Logs* starting on page 3-24

Settings immediately updated using Apply Now

You can enforce some configuration changes in the InterScan MSS console immediately by clicking **Apply Now**. The Apply Now button is displayed in the upper-left corner of the web console. When settings have been changed that need to be applied, the button's appearance changes to remind you to apply the changes.

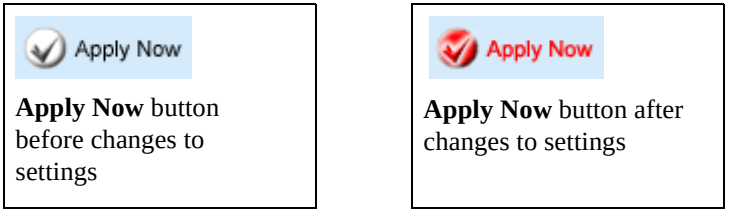


FIGURE 3-1. Apply Now button

The maximum amount of time that the program spends updating the settings is one minute. After this, if the update has not completed, InterScan MSS displays a message indicating that there is a problem with the service.

> **Note:** The scanning queue may grow temporarily after clicking Apply Now, because all InterScan MSS temporarily suspends scanning threads during the update process.

To enact the following configuration immediately, click **Apply Now**:

- All **Policy Manager**-related settings. For more information, see *Policy Management* starting on page 4-1
- Email and SNMP trap notification settings. For more information, see *Notification settings* starting on page 3-21
- **Security** settings. For more information, see *Updating InterScan MSS* starting on page 3-22

- All **Postfix** settings, except for the **Receiver > Settings > IP address** configuration where the InterScan MSS server is installed. These include:
  - **Connection** settings. For more information, see *Connection control* starting on page 3-9
  - **Connection Control** settings. For more information, see *Connection control* starting on page 3-9
  - **Relay Control** settings. For more information, see *Relay control* starting on page 3-10
  - **Domain-based Delivery** settings. For more information, see *Domain-based delivery* starting on page 3-12
  - **Message Limits** settings. For more information, see *InterScan MSS message settings* starting on page 3-13
- **Event Monitoring** settings. For more information, see *Configuring Event Monitoring settings* starting on page 3-20
- **Product License** settings (see *Activating Trend Micro Antivirus and eManager, and the Spam Prevention Solution (SPS)* starting on page 2-40)

What happens after clicking Apply Now?
1. All scanning threads are suspended 2. The policy settings in memory are updated 3. All scanning threads are resumed

Configuring Services

The Services section of the management console provides tools to configure InterScan MSS services. In the **Services** screen, InterScan MSS allows you to enable or disable SMTP and POP3 mail handling. This choice affects which adaptors are loaded during the initial service startup.

To choose the mail handling type:

1. In the navigation panel, click **Configuration** > **Services**.
2. Select SMTP or POP3 mail handling and click **Save**.

Enabling or disabling an adaptor

InterScan MSS provides tools for SMTP and POP3 scanning. You can choose which scan types are available.

SMTP

To enable the SMTP adaptor, click **Configuration** > **Services**, select **Enable SMTP**, and restart the InterScan MSS service. If you disable the SMTP adaptor, you cannot receive SMTP mail. In that case, only POP3 scanning will work.

POP3

To you enable POP3 scanning, click **Configuration** > **POP3** > **Settings**, and select **Enable POP3**. If you enable the POP3 adaptor, but disable scanning, InterScan MSS will receive POP3 mail but it is not scanned. If you disable the POP3 adaptor, and restart the InterScan MSS service, you will not receive POP3 mail. For more information on POP3 scanning see *Scanning POP3 messages* starting on page 3-13.

Configuring Postfix settings

Before InterScan MSS can start scanning messages to and from your network, you need to initially configure Postfix. InterScan MSS supports managing a restricted subset of Postfix settings from within the InterScan MSS interface. To enable InterScan MSS management of these Postfix settings, type **y** at the prompt.

Receiver settings

You can control the servers InterScan MSS will receive messages from, and the servers it will allow to relay. In addition, the IP address, SMTP greeting, and connection time-out settings in InterScan MSS are fully configurable.

Processing queue

Also in this screen is the **Processing Queue.** This is where InterScan MSS saves messages before scanning or delivering them. The default path is `/var/spool/postfix`.

Server settings

You need to specify the IP address and port to which InterScan MSS will bind. You can also configure the greeting message received by other SMTP servers after connection.

To configure the InterScan MSS IP address and SMTP greeting:

1. In the left frame, click **Configuration** > **Postfix** > **Receiver** > **Settings**.
2. Use the **IP address** (or preferably the FQDN) pull-down menu to select the IP address of the server where you have installed InterScan MSS.

Note: By default, InterScan MSS binds to all available network interfaces for this service. You may choose to bind to a specific network interface card when you choose a specific IP address from the pull-down menu.

---

3. In **Port**, enter the port number and in **SMTP server's greeting message**, type text into the associated text box.
4. Click **Save**.

Note: To apply the new settings, restart InterScan MSS.

Connections

Postfix accepts messages from other SMTP servers and, after processing is complete, passes these messages on. You can configure how InterScan MSS handles these connections.

To configure the InterScan MSS connection settings:

1. In the left frame, click **Configuration** > **Postfix** > **Receiver** > **Connections**.
2. In the **Connections** screen, you can configure:
   - The disconnection timeout period
   - The maximum number of simultaneous connections
3. Click **Save** and then **Apply Now**.

Connection control

For added security, you can limit which SMTP hosts are allowed to connect to the InterScan™ Messaging Security Suite server by specifying IP addresses or IP address ranges to lists which allow (or deny) access to your server. For example, you can block the IP address of an organization that has previously sent spam messages to you, or if you suspect spam senders of using the host as an open relay to relay spam.

To control which SMTP hosts are allowed to connect to InterScan MSS, select one of the following options:

- **Accept all, except for the following Deny Access list**
- **Deny all, except for the following Allow Access list**

To set connection privileges:

1. In the navigation panel, click **Configuration** > **Postfix** > **Receiver** > **Connection Control**.
2. In the **Connection Control** screen, choose whether you want to deny or allow access to a list of servers by selecting the appropriate option.
3. To configure the server lists, click the **Edit** link. When configuring the list, you can configure a single IP address or a range of IP addresses.
4. Click **Apply Now** in the top-left corner of the screen.

Relay control

You can control which computers InterScan MSS allows to relay messages through your server.

Unscrupulous people who attempt to relay messages through an SMTP server are a common challenge for mail administrators. Spam senders may relay their messages through an unsuspecting company's mail server to hide their identity, give the message an air of respectability, or to use other people's bandwidth resources.

Note: When configuring relay control, you can use the wildcard *. For more information about using the wildcard, see *Using the "*" Wildcard In Routes* starting on page 4-24.

InterScan MSS manages relay control by:

- Restricting relay to specific local domains: InterScan MSS allows all hosts to relay mail to a specific list of destinations (**Allowed Relay Destinations**). Enter only the domain names of mail hosts used by your organization.
- Allowing exceptions based on:
  - **Host only**
  - **Same subnet as the hos**t (default)
  - **Same IP class as the host**
  - **Specified IP addresses**

InterScan MSS only allows hosts that you specify (**Permitted Senders of Relayed Mail**) to relay messages to hosts not in the **Allowed Relay Destinations** list.

Essentially, only those hosts in the **Permitted Senders of Relayed Mail** list can use the InterScan MSS server to relay messages to any domain or use InterScan MSS as an open relay. Enter the names of mail hosts that you trust to use their relay privileges appropriately and send authorized outbound email from internal mail servers.

Note: Leave the **Permitted Senders of Relayed Mail** list empty to prevent all servers from relaying messages to the Internet using InterScan MSS.

To set relay privileges:

1. In the navigation panel, click **Configuration** > **Postfix**> **Receiver** > **Relay Control**.
2. Enter the **Allowed Relay Destinations** (the hosts within your intranet)
3. Enter the **Permitted Senders of Relayed Mail** (mail hosts you trust and want to allow to relay messages to the Internet).
4. Click **Save**, then click **Apply Now** in the top-left corner of the screen.

Configuring delivery settings

InterScan MSS is a gateway product that routes mail to Postfix to resolve the final destination. You can configure whether InterScan MSS performs this process, based on the recipient's domain name, using **SmartHost**.

Domain-based delivery

InterScan MSS routes email based on the recipient's domain. The routing method is to forward to **SmartHost**. When you have multiple **SmartHosts** on the list, InterScan MSS performs load balancing to make the best use of network and server resources.

To view the current delivery methods:

1. In the navigation panel, click **Configuration** > **Postfix** > **Domain-Based Delivery**.
2. The **Domain-Based Delivery** screen shows how InterScan MSS and Postfix will process mail destined for a specific domain. To view or change a given domain's delivery method, click **Edit** in the **Details** column.

To create a new delivery method:

1. In the **Domain-Based Delivery** screen, click **Add**.
2. Type a name for the destination domain.
3. Type the destination domain server IP address
4. Type the destination domain server port number.
5. Click **Save**.

   The order that server names appear in the SMTP server list dictates priority.

InterScan MSS message settings

To prevent message delays, you can limit the message size or the number of message recipients that InterScan MSS will process. InterScan MSS will not deliver messages if they exceed the maximum limits that you configure.

To set message limits:

1. In the navigation panel, click **Configuration > Postfix** > **Message Limits**.
2. Select the items to limit and enter the value.

   Note: If you do not want to set a limit, clear the item or type a "0" in a field. Setting the limit to "0" is equivalent to setting no limit. Therefore, if you select an item, type "0", and click **Save**, the window refreshes to show the item not selected.

3. Click **Save**, then click **Apply Now** in the top-left corner of the screen.

Note: If you set a maximum number of recipients for messages, InterScan MSS accepts messages only to the number of recipients specified per session. Messages in excess of the limit will be rejected. The sending SMTP server is then expected to retransmit the remaining recipients in another session.

Scanning POP3 messages

In addition to SMTP traffic, InterScan MSS 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, for example, Hotmail® or Yahoo® accounts that provide POP3 access, using mail clients on their computers. This can create points of vulnerability on your network if the messages from those accounts are not scanned.

Understanding POP3 Scanning

The InterScan MSS POP3 scanner acts as a proxy, positioned between mail clients and POP3 servers, to scan messages as the clients retrieve them.

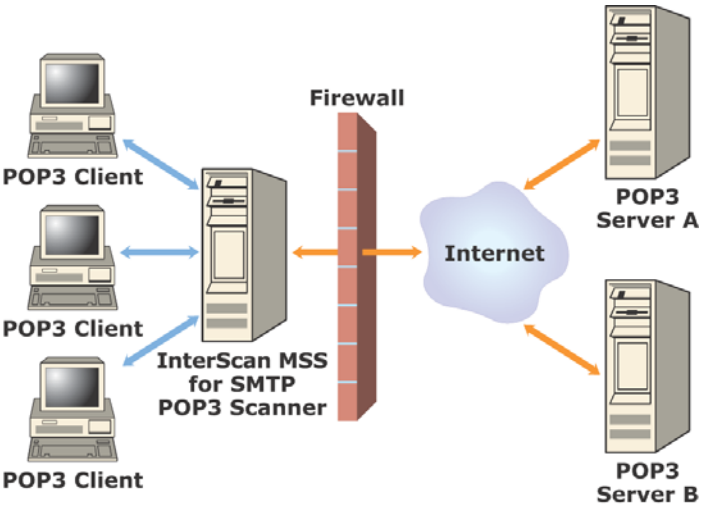


FIGURE 3-2. How POP3 scanning works

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

You can set up the following connection types:

- A **Generic** connection allows you to access different POP3 servers using the same port—typically 110—the default port for POP3 traffic.
- **Dedicated** connections access the POP3 server using a specified port. Use these connections when the POP3 server requires authentication using a secure log-on, such as APOP or NTLM.

Requirements

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

Your network users have to manually configure a mail client. For more information on this task, see *Configuring email clients* starting on page 3-17.

Settings

Before InterScan MSS can begin scanning POP3 traffic, you will need to enable POP3 Scanning and perform an initial configuration.

To enable POP3 message scanning:

1. In the navigation panel, click **Configuration** > **POP3** > **Settings**.
2. Select **Enable POP3 Scanning**.
3. If you have installed InterScan MSS on a server that has more than one network card (NIC), select the IP address of the card that you want to retrieve POP3 traffic on behalf of your mail clients.

Note: If a POP3 message triggers a filter that stops message delivery, InterScan MSS delivers a message containing the **Status Message Text** instead. The action performed on the undelivered message depends on the policy actions associated with the filter, such as **delete**, **forward**, or **quarantine**.

---

4. Click **Save**, then click **Apply Now** in the top-left corner of the screen.

Users must update their mail client configurations to retrieve email through the InterScan MSS POP3 proxy with these settings.

Connections

You can specify the ports on the InterScan MSS 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 view the POP3 connections currently set up on your server:

1. In the navigation panel, click **Configuration** > **POP3** > **Connections**.
2. The POP3 server and port connections that have already been set up appear in the table. Click the **view** link to see a specific connection's properties.

To add a new POP3 connection:

1. In the navigation panel, click **Configuration** > **POP3** > **Connections**.
2. Click **Add**.
3. The port the InterScan MSS server uses to accept POP3 traffic for that connection shows under **Inbound POP3 Port**. Type the port that you want to use, if different.
4. The properties of the POP3 server show under **POP3 Server**. You can select **Any POP3 server requested by user** to set up a generic connection or select a **Server name** under **Specific POP3 server** to configure a dedicated connection.
5. Click **Save** to save your configuration changes, then click **Apply Now** in the top-left corner of the screen.

   Once you have created or modified a generic connection, users must adjust their configuration to reconfigure their mail clients to retrieve email through the InterScan MSS POP3 proxy with the updated settings.

To delete a POP3 connection:

1. In the navigation panel, click **Configuration** > **POP3** > **Connections**.
2. Select the connection that you want to delete.
3. Click **Delete**.

Configuring email clients

After you install InterScan MSS and configure POP3 scanning, your users must configure their POP connection settings to access your POP3 server through the InterScan MSS proxy.

Setting up generic connections

For generic connections that support most POP3 servers, assume the following account information is provided as the current client POP configuration:

- Incoming mail (POP3) server: `pop.domain.com`
- Account name: `John_Smith`

For example, assume the **Inbound POP3 IP Address** used by InterScan MSS is 123.123.123.12.

To enable POP3 mail retrieval and scanning, change the settings to the following:

- Incoming mail (POP3) server: `123.123.123.12`
- Account name: `John_Smith#pop.domain.com`

Note: When trying to access a POP3 server that uses a port other than what is specified in the InterScan MSS generic connection port setting, append an extra "#" separator and add the port. For example, if the POP3 server uses port 120, when InterScan MSS is set to use 110, the account name is **John_Smith#pop.domain.com#120**.

Setting up dedicated connections

If the actual POP3 server that you are trying to connect to is listening on a port number different from the one you entered in the **Inbound POP3 Port** for your clients, type this POP3 server port number into the **Port number** field after the server name.

To use the dedicated connection, modify your mail client in the following ways:

- Change the POP3 server port in your mail client's settings to the port used by InterScan MSS as the **Inbound POP3 Port**.
- Modify the incoming mail POP server to use the InterScan MSS proxy IP address.

Note: The account name does not change since the actual POP server is referenced in the InterScan MSS dedicated connected settings.

- Incoming mail (POP3) server: `pop.domain.com`
- Account name: `John_Smith`

For example, assume the **Inbound POP3 IP Address** used by InterScan MSS is 123.123.123.12.

To enable POP3 mail retrieval and scanning, change the settings to the following:

- Incoming mail (POP3) server: `123.123.123.12`
- Account name: `John_Smith#pop.domain.com`

Note: When trying to access a POP3 server that uses a port other than what is specified in the InterScan MSS generic connection port setting, append an extra "#" separator and add the port. For example, if the POP3 server uses port 120, when InterScan MSS is set to use 110, the account name is **John_Smith#pop.domain.com#120**.

Using dedicated connections

If the actual POP3 server that you are trying to connect to is listening on a port number different from the one you entered in the **Inbound POP3 Port** for your clients, type this POP3 server port number into the **Port number** field after the server name.

To use the dedicated connection, modify your mail client in the following ways:

- Change the POP3 server port in your mail client's settings to the port used by InterScan MSS as the **Inbound POP3 Port**.
- Modify the incoming mail POP server to use the InterScan MSS proxy IP address.

  The account name does not change, since InterScan MSS references the actual POP server in the dedicated connected settings.

Configuring directories

InterScan™ Messaging Security Suite uses directories on the local machine to store messages that are queued for processing.

Understanding queues

The following default directories are used for postpone and processing queues:

- Postpone queue:

  `/opt/trend/imss/queue/postpone`

- Processing queue:

  `/var/spool/postfix`

During normal operation, InterScan MSS temporarily stores most of the messages for scanning and delivery in the `mqueue` folder. You can change the default location of this folder.

To change the default paths:

1. In the left frame, click **Configuration** > **Directories**.
2. Type the paths that you want to use for the **Postpone Queue**.
3. Click **Save**, then click **Apply Now**.

Configuring Event Monitoring settings

InterScan MSS can proactively notify an administrator if conditions arise that threaten to disrupt mail processing or constitute a security risk.

InterScan MSS notifies the administrator if any of the following conditions arise:

- The result of a scheduled update attempt (successful or unsuccessful)
- Stopped scanning service
- Running out of disk space in the processing queue folder that might hamper mail processing
- If the mail queue exceeds a specified number of messages.

To configure events for which InterScan MSS should provide notification:

1. In the left frame, click **Configuration** > **Event Monitoring**.
2. Select the fault conditions, and enter the values.
3. Select the notification method(s).
4. Click the **Edit message** link next to the notification method(s) that you want to use and configure the messages for the different events.

   You must configure the notification settings for the method(s) that you choose to use.
5. Click Save.

Note: InterScan MSS System Monitor applies changes to the updated Event Monitoring settings when you click Save.

Notification settings

InterScan MSS can notify you through email or SNMP trap when it detects a virus, when a policy is updated, or if the system requires attention.

Note: The `imssd` parent process and two of the child processes run as root, but all of the other child processes run as "imss". This child process runs as root because it is playing the role of delivering the notification, and therefore, must have root permission.

To configure notification settings:

1. In the navigation panel, click **Configuration** > **Event Monitoring** > **Notification Settings**.
2. Configure the settings for all of the notification methods that you want to use—email or SNMP Trap.
   - If email notification messages contain non-English characters, enter the Preferred charset.
   - Typing a "0" in any field is the same as not setting a limit or selecting a check box.
   - Using SNMP trap notification requires a simple network management protocol (SNMP) server to receive the SNMP trap. InterScan MSS uses trap type to distinguish between different events.

Can I set my notification server as localhost?

Since InterScan MSS is an SMTP server, you may be wondering if you can use it to send notification messages. It's possible, but it's not recommended.
Since the default settings prohibit any relay through the InterScan MSS server, you would have to add this server's IP address to the *Permitted Senders of Relayed Mail*. The risk, however, is that the **System Monitor** also uses the notification SMTP server to inform the administrator about fault conditions with your software. If the InterScan MSS server is down, no notification from the **System Monitor** can be sent.

3. Click **Save** when finished, then click **Apply Now** in the top-left corner of the screen.

Updating InterScan MSS

InterScan MSS blocks viruses and spam email by comparing a file's binary pattern and message content to data stored in the virus pattern file and spam pattern files. To maintain the highest level of protection against the latest virus and content threats, InterScan MSS needs to regularly update your antivirus and spam pattern files.

Trend Micro updates its virus pattern file, often several times a week, in response to newly released viruses. In addition, Trend Micro periodically updates the scan engine, the component that compares a file's binary structure with the virus pattern file. This engine detects virus-like behavior and cleans viruses when it detects them. Trend Micro also periodically updates the heuristic spam rules used by Spam Prevention Solution.

Note: InterScan MSS retains all old virus pattern files on the server and does not delete them after update. See *Rolling back an update* starting on page 3-24 for information about undoing a pattern update.

Configuring proxy settings

If you use a proxy server to connect to the Internet, configure your server and authentication settings before attempting an update.

To configure update proxy settings:

1. In the navigation panel, click **Configuration** > **Update** > **Proxy Settings**.
2. Select **Use a proxy server** and enter the proxy server's name, port, and authentication information.
3. Click **Save**. InterScan MSS immediately applies the new proxy settings in the **InterScan MSS Scheduler**.

Note: As a security precaution, the proxy password is sent only once from the management console to the InterScan MSS server.

Using on-demand update (Update Now)

To update the virus pattern and spam pattern file:

1. In the navigation panel, click **Configuration** > **Update** > **Update Now**.
2. Select the components that you want to update. InterScan MSS shows newer components, if present, with a red Update Now!
3. To update from a location other than the Trend Micro Active Update server, select **Other Internet source** and type the URL in the associated text box.
4. When you have finished, click **Update Now**.

Scheduling updates

InterScan MSS can automatically download updates hourly, daily, or weekly. If your network has limited Internet bandwidth, you can configure updates for a time when network load is low.

To configure a scheduled update:

1. In the navigation panel, click **Configuration** > **Update** > **Scheduled Update**.
2. Select **Enable Scheduled Update** at the top of the screen and choose the components that you want to download.
3. Configure the time and update interval.
4. Modify the update URL, if needed.
5. Click **Save**.

Note: InterScan MSS immediately applies new **Scheduled Update** settings to the **InterScan MSS Scheduler** after you click Save.

Rolling back an update

After updating to a new virus pattern file, InterScan MSS keeps the old pattern files on the server. You will need to manually delete older files that you no longer need from time to time, but Trend Micro recommends keeping the last three versions of this file, in case a pattern file becomes corrupted and you need to roll back.

Note: The virus filter always uses the pattern file with the largest pattern file number.

To roll back to a previous virus pattern file:

1. Note the version of the virus pattern file that you are currently using.
2. Stop InterScan MSS service.
3. Delete or rename the file `$IMSS_HOME/lib/lpt$vpn.###`, where ### is three digits representing the pattern file version.
4. Verify that there is another virus pattern file in the `$IMSS_HOME/lib` path where the pattern version is less than the one you deleted.
5. Restart the InterScan MSS service.

Working with Logs

Logs store important information about security and program events for InterScan MSS. You can use the logs to monitor InterScan MSS performance, or to troubleshoot message processing.

Viewing logs

1. In the navigation panel, click **Configuration** > **Logs**
2. Choose one of the following:
   - **Virus Logs**
   - **eManager Logs**
   - **Program Logs**
3. Enter the log parameters for which you want to search.
4. Click **View Logs**.

Log maintenance

You can configure the logging behavior of InterScan MSS, including the level of detail, the location of the log database, the maximum size of all log files and the amount of time that log entries will be retained.

Note: If you do not regularly remove old log files from your log directory, and your InterScan MSS server processes high volumes of messages, the log file will consume more and more disk space.

1. In the navigation panel, click **Configuration** > **Logs** > **Log Maintenance**.
2. Select which log level (**Normal**, **Detailed**, or **Diagnostic**) you want to save to the log file.

   Normal: The standard level of detail. This level provides the basic information needed by an administrator for daily monitoring and maintenance.

   Detailed: A higher level of detail. All InterScan MSS processes write detailed message flow information to the log, including: telnet session information, the policy matched, the filter executed, and the outcome triggered.

   Diagnostic: The most complete information on each transaction. Diagnostic level logs include all information from the detailed level, plus SMTP routing information, and the route match weights that determined which policy applied.
3. In **Directory to store logs**, type the directory path where you want the logs kept.
4. In **Days to keep logs**, type the number of days you want InterScan MSS to retain logs.
5. In **Maximum size to store**, type the maximum amount of space you want to allow log files to consume. When the total size of the logs exceeds this threshold, InterScan MSS deletes the oldest log files.

   Note: The default is 0, which allows an unlimited maximum log size.
6. Click **Save**.

Restart the InterScan MSS service to apply your new log settings.

Setting the InterScan MSS password

You can view the InterScan MSS Web console locally through a Web browser from the machine where you installed the program, or remotely across the network. To prevent unauthorized access, Trend Micro recommends that you configure a password immediately after installation.

To set the console password:

1. Click **Configuration > Password**.
2. Type the current password, if any, in the space provided.
3. Type your new password.
4. Confirm your new password.
5. Click **Save**.

Modifying your XML file directly

WARNING! Backup the XML file before modifying it.

To manually modify your XML file:

1. Use the S99ISIMSS script to shut down the InterScan MSS daemon, aphost, and other daemons that use the regserver.
2. Backup the original XML file.

   If you perform a backup, you only need to backup .xml (not the .bak or .redo) files.
3. There are several alternatives:
   - Use the command line tool provided by Trend Micro to modify the XML file contents. Check the manpage for more information on the command line tool.
   - Use a conversion tool (or a third-party tool) to convert the XML file to a user-familiar text format. You can then modify the text file and convert it back to the .xml file.
4. Use the S99ISIMSS script to start the regserver daemon. (This script is in the InterScan MSS installation directory.)

Chapter 4

Policy Management

This chapter explains how to set up policies for different individuals and groups in your organization to enforce your antivirus and content management goals.

Topics include:

- How the **Policy Manager** works
- Using the InterScan™ MSS built-in filters
- Defining address groups
- Defining and using filter actions
- Setting up quarantine directories
- Understanding the **Global Policy**
- Creating a sub-policy
- Setting the order of filter execution within a sub-policy

How the policy manager works

A policy is a set of rules applied to messages based on sender and recipient email addresses. InterScan MSS's policies can filter and reduce many security and productivity threats to your messaging system.

A policy has the following components:

- The **Route** is the set of sender and recipient email addresses to which the policy is applied. Wildcard expressions can be used to simplify route configuration.
- The **Filter** is a rule or set of rules that apply to a specific route. InterScan MSS contains predefined filters you can use to combat common virus and content threats. In addition, you can define your own filters.
- The **Action** is the action that InterScan MSS should take if the filter conditions are met or not met. Depending on the filter result, a filter action is performed that determines how the message is finally processed. .

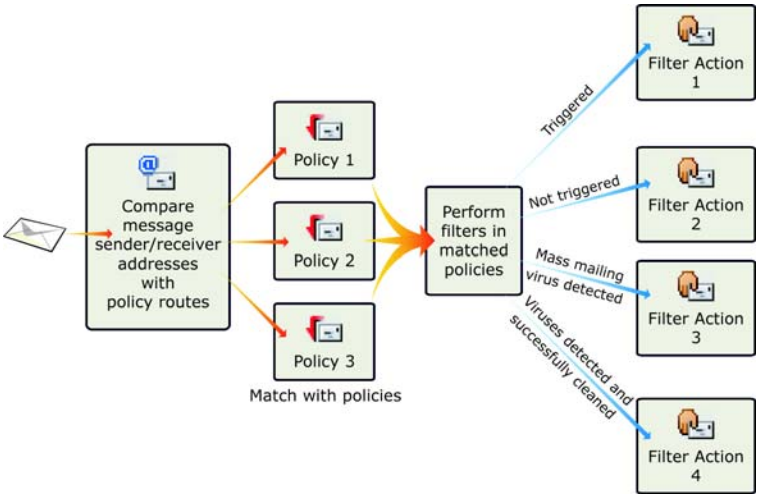


FIGURE 4-1. Simplified Policy Manager process flow

Viewing installed filters

Filters are tests that analyze messages and attachments for viruses or content that you want to block from your network. InterScan MSS contains seven default filters—one that uses the Virus filter and six that use the eManager filter.

If you have activated SPS you also have access to heuristic filters, which filter email based on a complex set of rules and patterns. More information about SPS filters is in *Filtering Content with the Spam Prevention Solution Filter (SPS)* *starting on page 7-1*.

To view the filters that you can use as the building blocks for your policies, in the navigation panel, click **Policy Manager**. The filters are listed in a table at the bottom of the **Policy Manager** screen.

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 applied to these groups would be the following:

Address Groups	FINANCIAL	JOBSEARCH	VBSCRIPT
All Executives	Not applied	Applied	Applied
All HR Department	Applied	Not applied	Applied

Address Groups	FINANCIAL	JOBSEARCH	VBSCRIPT
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 InterScan MSS, 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 to apply the same email usage policy to every address in the group.

Defining an Address Group

To define an address group:

1. In the navigation panel, click **Policy Manager > Address Group**. The **Address Group** screen shows existing address groups.
2. Click **Add**.
3. In the **New Address Group** screen, type a descriptive name for the address group and enter the email addresses of individuals who will be in the group.
4. Click **Save**. You are returned to the **Address Group** screen. Your newly created group appears in the list.

Modifying an address group

To modify an existing address group:

1. In the navigation panel, click **Policy Manager > Address Group**. Click the **details** link for the group you want to modify.
2. To remove an address from the group, select it in the **Address group** list and click the (-) button. Add new addresses by typing it in the **Email Address** field and clicking the add button.
3. Click **Save**.

Deleting an address group

To delete an address group:

1. In the navigation panel, click **Policy Manager > Address Group**.
2. Select the address group and click **Delete**. To delete all defined address groups, select **All** at the top of the column and click **Delete**.
3. Click **OK**.

Note: If an address group has **in use** in the right-hand column, then this address group is currently being used in a route and cannot be deleted while the route exists.

Importing an Address Group from a File

InterScan MSS supports importing addresses from files in a local drive on the InterScan MSS server.

To import address information:

1. In the navigation panel, click **Policy Manager** > **Address Group**.
2. To import addresses to an existing group, click **Details** under the **Edit** column.
3. To create a new address group from imported addresses, click **Add** and enter a name for a new group.
4. Click **Import**.
5. Type the path to the file you want to import.

Note: You cannot import address list information from a remote computer. Addresses cannot be imported using HTTP upload or by typing a UNC path. The file must be on a drive local to the InterScan MSS server.

---

6. Select a file type.

Note: Both comma-separated values (CSV) and LDAP Data Interchange Format (LDIF) are supported. If you select the CSV file type, it has to be in the format described in Address list format starting on page 4-6.

---

7. Choose whether to merge the imported addresses or overwrite.
8. Click Import

If you are remotely viewing the InterScan MSS console using a browser, first copy the text file into a shared directory on the InterScan MSS server. Then enter the file path and name information into the screen relative to the InterScan MSS server.

Address list format

To import an address group from a text file, each line in the file must contain a single email address followed by a carriage return character.

A valid text file for importing an address list would appear as below:

```
Daniel@trendmicro.com
Jennifer@mountainview.gov
SomeDude@yahoo.com
...
```

Using filter actions

The filters employed by the InterScan MSS policies perform tests on messages and their attachments.

For filters that use the Virus filter, the following results are possible:

- Messages with potentially malicious compressed attachments (IntelliTrap)
- Mass mailing virus detected
- Virus or spyware/grayware detected but some/all were not cleaned or deleted
- Joke program attachment detected
- Virus(es) detected and successfully cleaned
- Virus scanning aborted—message may contain viruses
- Password-protected file detected (not scanned)
- Virus or spyware/grayware detected and successfully cleaned or deleted
- Virus(es) detected but some/all were not cleaned
- No virus detected

For filters using the eManager filter , there are only two possible results:

- Triggered
- Not triggered

For each possible result of the filter that you are using, define the filter action that you want to take.

Using predefined filter actions

InterScan MSS provides default filter actions. In addition to creating your own filter actions, you can use the default actions in your policies.

They are:

- **Deliver**, which delivers the message normally
- **Delete**, which deletes the message
- **Delete and Notify**, which deletes the message and notifies the administrator
- **Deliver and Notify**, which delivers the message and notifies the administrator
- **Postpone and Notify**, which postpones the delivery of the message until after midnight and notifies the administrator
- **Quarantine and Notify**, which sends the message to the default **Quarantine Area** and notifies the administrator

---

Note: In filter actions that notify the administrator, the notification is sent to the email address configured for notifications. For more information about setting or changing this address, see *Notification settings* starting on page 3-21.

- **Quarantine**, which sends the message to the default **Quarantine Area**
- **Tag and Deliver**, which prepends the message subject with “Spam:” The tag and deliver action is only available for the SPS heuristic filter

Understanding the components of a filter action

A filter action is composed of the following components:

- **Processing Action**
- **Archive**
- **Notification**

Note: A filter action can contain any number of archive and notification actions but only one (or no) processing action. If you do not configure the processing action, the message is delivered as usual.

Processing action

You can choose to postpone the delivery, quarantine the message to a directory on your local disk, delete the message, or forward the message to another email address. These four actions mean the message will not be delivered to the addressee at this time. You can also choose to deliver the message normally.

Archive

Messages can be archived to a local directory or a mail account. You can archive the message in its original form, archive the message after it is modified by a filter, (for example, you can archive the message after InterScan MSS cleans any viruses from the attachment), and/or have a disclaimer added to the message body.

Notification

Notifications can be sent to an email address or an SNMP trap. Email notifications can be sent to the original email sender, the recipient, the administrator or any other email address that you choose. **Notification** is similar to **Archive** because you can attach the message in its original form or send the message that was modified by the virus or eManager filters.

Managing filter actions

Filter actions are based on whether the filter is triggered.

Creating a new filter action

To create a new filter action:

1. In the navigation panel, click **Policy Manager** > **Filter Action**.
2. In the **Filter Action** screen, click **New Filter Action**.
3. Enter a name for the filter action and click **New Item**.
4. In this screen, enter a short description and select **Processing Action**, **Archive**, or **Notification**. Click **Next**.
   - For **Processing Action**, select how you want the message to be processed. The options are **Quarantine**, **Postpone**, **Forward**, **Delete**, or **Deliver** and click **Next**.

     Note: When you configure a forward action, enter an email address in the **From** sender field for the message. InterScan MSS does not perform any validation on this address. You can enter anything, provided it is accepted by your mail server and the **From** field does not exceed 255 characters.

   - For **Archive**, select whether to archive the message to a local directory or a mail account.
   - For **Notification**, type the text of the notification message and specify the parties who will receive the notification and the subject line of the message. You can also attach the message—a copy of the original or a copy of the message after it has been modified by InterScan MSS.

Note: For more information about changing your notification settings, see *Notification settings* starting on page 3-21.

- Click **Next**. A summary page loads, displaying the parts of the filter action that you configured. To add another **Processing Action**, **Archive** or **Notification** to the filter action, repeat steps 3 and 4 until you have finished. Remember, a filter action can contain multiple **Archive** and **Notification** items, but only one **Processing Action** is allowed.

Modifying a filter action

To modify an existing filter action:

1. In the navigation panel, click **Policy Manager > Filter Action**.
2. In the **Filter Action** screen, click the link of the filter action you want to modify.
3. A list of **Processing Action**, **Archive**, and **Notification** items used in the selected filter action is shown. Click **Edit** to modify an item. To delete an item, select the item and click **Delete**.
4. Click **Finish**.

Deleting a filter action

To delete a filter action:

1. In the navigation panel, click **Policy Manager > Filter Action**.
2. In the **Filter Action** screen, select the filter action that you want to remove and click **Delete**.

Note: If a filter action has **in use** in the right column, then this filter action is currently being used by a filter and cannot be deleted while the filter exists.

Using quarantine areas

Quarantine areas are directories on the InterScan MSS server where messages can be moved as the result of a processing action.

You may want to quarantine messages to:

- Reduce the chance of important messages being deleted (in case they are erroneously flagged by the eManager or heuristic spam filter).
- Review messages that trigger content filters to determine the severity of the policy infraction.
- Keep a record of oversized messages (in case they contain important information that is urgently needed by the recipient).
- Maintain, for disciplinary purposes, evidence of an employee's continued misuse of your organization's messaging system.

Managing quarantine areas

Quarantine areas serve as storage for messages that trigger filters to facilitate further investigation.

Adding a quarantine area

To add a quarantine area:

1. In the navigation panel, click **Policy Manager** > **Quarantine Area**.
2. In the **Quarantine Area** screen, click **Add**.
3. Enter a descriptive name for the **Quarantine Area** in the program and type a local path to the machine on which InterScan MSS is installed.
4. To automatically delete quarantined messages after a set period of time, select this option at the bottom of the screen and type the number of days quarantine items should be kept.

   Note: Quarantine items can be saved up to 99 days.

5. Click **Save**. The **Quarantine Area** screen loads and displays the new quarantine area.

Changing a quarantine area

To change the location of a quarantine area:

1. In the navigation panel, click **Policy Manager > Quarantine Area**.
2. In the **Quarantine Area** screen, click **Edit** next to the **Quarantine Area** that you want to modify.
3. Change the **Name** and/or **Directory**, or change the number of days that you want quarantined items to be kept.
4. Click **Save**.

What happens to quarantined items in the old folder?
Changing the quarantine location only affects items quarantined after the change. Any messages in the old quarantine directory must be manually copied to the new directory or manually deleted.

Managing quarantined messages

To manage the contents of a quarantine area:

1. In the navigation panel, click **Policy Manager > Quarantine Area**.
2. In the **Quarantine Area** screen, click **view** next to the **Quarantine Area** that you want to manage.
3. In the **Quarantine Area** screen, select one of the following options:
   - **Reprocess** messages to apply the policies that have been configured for the message's route. You may want to reprocess messages if a content filter that was too strict quarantined innocent messages. After you have changed the content filter's properties, reprocess these messages.
   - **Deliver** the message without further processing

Note: Messages in a quarantine area may contain viruses or malicious code if they were malformed or if they were quarantined by a filter that executed before they were scanned by the virus filter. Selecting **Deliver** bypasses antivirus scanning and is not recommended.

   - **Delete** the message
   - **Reprocess All** to reprocess all the messages in the quarantine area, reapplying the appropriate filters to each message

- **Deliver All** to deliver all the messages in the quarantine area, without reapplying the appropriate filters to each message

Note: Messages in a quarantine area may contain viruses or malicious code if they were malformed or if they were quarantined by a filter that executed before they were scanned by the virus filter. Selecting **Deliver All** bypasses antivirus scanning and is not recommended.

- **Delete All** to delete all the messages in the quarantine area

4. When you have finished, click **Return** to go back to the **Quarantine Area** screen.

Deleting a quarantine area

To delete a Quarantine Area:

1. In the navigation panel, click **Policy Manager** > **Quarantine Area**.
2. In the **Quarantine Area** screen, select the quarantine area that you want to remove.
3. Click **Delete**.

Deleting the **Quarantine Area** in the InterScan MSS console only prevents it from being available to the program as a quarantine area. If you want to delete the folder, you must do so manually. All quarantined messages remain in the folder.

Note: If a quarantine area has **in use** in the right column, then it is being used in a filter action and cannot be deleted.

Querying quarantine areas

InterScan MSS includes a search function to query a quarantine area for messages that fit your criteria.

To query a quarantine area:

1. In the navigation panel, click **Policy Manager** > **Quarantine** > **Query**.

In the **Query** screen, select the quarantine area and enter the criteria for which you want to search. You can perform a case-sensitive search by selecting **Enable Case Sensitive Search**.

Note: Wildcards, such as "*" are not supported when querying a quarantine area.

2. Click **Query**.
3. The results of the query will be displayed.

Acting on quarantined messages

You have the option to **Reprocess**, **Deliver** or **Delete** the messages that have been quarantined. Select individual messages for action, or choose to reprocess, deliver, or delete all the messages in the quarantine area.

- **Reprocess** sends messages back through the active filters for reevaluation.
- **Delete** removes the messages from the quarantine area.
- **Deliver** bypasses all filtering and delivers the messages to the recipient.

WARNING! Choosing **Deliver** could cause virus-infected, malformed, or offensive messages to be delivered. Do not choose this option unless you are sure that the messages you are delivering are safe.

The Global Policy

The **Global Policy** includes tasks that are applied to all of the messages flowing through the InterScan MSS server. In other words, the **Global Policy**'s route is the set of all messages from "*" and going to "*".

After installing InterScan MSS, the **Global Policy** contains one enabled **Antivirus Filter**, named **Virus and potentially malicious code**, which scans all messages and message attachments using the virus pattern file. If you have activated SPS, it will also contain an **SPS Spam Filter**

In addition, the **Global Policy** contains the following disabled content management filters:

- **Profanity**: Filters common swear words
- **Racial Discrimination**: Filters racist slurs
- **Sexual Discrimination**: Filters sexist and homophobic language
- **Hoaxes**: Filters expressions found in common hoaxes that circulate using Internet email
- **Chainmail**: Filters chain email messages that encourage users to forward to everyone they know
- **Love Bug**: Filters expressions that appear in the email message that harbors the infamous auto-spamming ILOVEYOU virus
- **Block HTML Script Messages**: Filters HTML messages with embedded scripts, like JavaScript or VBScript

For each filter, there are **Edit** buttons for the following:

- **Filter Type**: Allows you to view and change the filter's properties

---

WARNING! Most people find the keywords used in the **Profanity**, **Racial Discrimination** and **Sexual Discrimination** filters offensive. These words are displayed only after clicking the **Filter type Edit** button, so that administrators can see the exact properties of the filter.

- **Filter Availability and Status**: Allows you to change whether the filter is available for a policy's definition, whether it is active, and whether the filter can be overruled by another filter in a sub-policy.

- **Filter Action**: Shows the action taken, depending upon the outcome of the filter (whether a message triggers the test performed in the filter)

Overruling a filter

When you create an antivirus filter in the global policy or a parent policy, this filter is inherited by the sub-policy. When the sub-policy also has a **Virus** filter, in the filter availability and status column, the **Overruled** status is displayed. **Overrule** means that this inherited Virus filter will not be executed. Rather, the Virus filter in the sub-policy is used.

Filter type

When viewing the **Global Policy** screen, clicking **Edit** under the **Filter Type** column displays the filter's properties.

- For all of the filters that use the **Advanced Content Filter**, you can view the filter properties, including the message parts that will be scanned and the keyword expressions that will be searched.
- For more information on adjusting the **SPS Spam Filter** settings, see *Heuristic spam filter settings* on page 4-19.

Filter availability and status

Every filter has a set of properties that control whether it can be used in any policy, whether it is active in the current policy, or whether it can be overridden by a sub-policy. These properties are called **Filter Availability**, **Filter Status** and the filter's **Override Property**.

Filter availability

To use a filter in your policy definitions, set it as **Available**. Setting a filter as **Disabled** means that it is not available for use in any policy.

Filter status

To make a filter part of a policy, set it as **Active**. A filter that is **Inactive** will not be used in the policy.

Override property

You need to decide whether the filters in sub-policies will override the filter configuration in their parent.

Consider the following example:

- A **Message Size Filter** in the **Global Policy** that postpones the delivery of messages greater than 2MB during business hours
- A **Message Size Filter** in the sub-policy that postpones the delivery of messages greater than 5MB during business hours

If you set the **Global Policy**'s filter as **Allow filter to be overwritten by a sub-policy**, then the sub-policy's filter takes precedence and 5MB messages are postponed. On the other hand, if you set the **Global Policy**'s **Message Size Filter** as **Do not allow filter to be over-written**, then it takes precedence and all messages greater than 2MB are postponed.

Note: The **Override Property** applies only to the eManager filters. When both the **Global Policy** and a sub-policy contain an **Antivirus Filter**, the filter in the sub-policy is always executed first. In other words, selecting **Do not allow filter to be overwritten** for the **Global Policy**'s **Antivirus Filter** is redundant.

Heuristic spam filter settings

The filter status and availability settings for the heuristic spam filter work differently than those settings for other filters. You may set this type of filter to active or inactive, overridable or not overridable, and can choose whether to maintain the **Approved Senders** or **Blocked Senders** list settings for subpolicies.

Heuristic Spam Filter Status

For heuristic spam filtering, the status can be either **Active** (applied to the policy) or **Inactive** (not applied).

Maintaining Approved/Blocked Sender lists

Selecting **Maintain Approved/Blocked Senders inheritance while inactive** keeps the Approved or Blocked Senders list entries available to subfilters, even if the parent filter is inactive.

To change the filter status, override, or Approved or Blocked Senders inheritance settings:

1. Click the **Edit** button next to the heuristic spam filter that you want to change.
2. Adjust the filter settings as desired.
3. Click **Save**.

Understanding the available filters

InterScan MSS by default is configured with one antivirus and six content management filters that you can customize and use in your policies.

Antivirus filter

The **Antivirus Filter** uses pattern-matching technology to scan messages and their attachments for viruses. Configuration options include the file types to scan, compressed file scanning behavior, the action if viruses are found, and inserting disclaimers into the message body. For more information about **Virus Filter** configuration options, see *Using the Antivirus Filter* starting on page 5-1.

eManager™ filters

The following filters use the eManager filter's content scanning engine. Detailed information about each is available from *Filtering Content with the eManager™ Filtering Tools* starting on page 6-1.

Note: If you installed a trial of the heuristic spam filter, the filter is shown during the evaluation period. If you do not upgrade to the full version, all heuristic spam filter functionality ceases.

- The **Advanced Content Filter** allows you to check the message header (or specific fields within the header), the body, or the attachment. It supports complex expressions and synonym checking. For detailed information, see *Filtering messages based on size* starting on page 6-2.
- The **Message Attachment Filter** is used to block message attachments at the SMTP gateway, including blocking them based on their MIME content-type. You can block by filename (supports wildcards), file type or MIME content-type. For more information, see *Creating or modifying the filter* starting on page 6-10.
- The **General Content Filter** is a simplified content and attachment filter that filters messages by subject line, keyword(s), attachment file size or extension. For more information, see *Filtering content using the general content filter* starting on page 6-14.
- The **Message Size Filter** allows precise control over attachments entering the SMTP gateway. The filter supports an activation schedule to block large attachments from your network during business hours but allowing them during off-peak periods, such as nights or weekends. See *Filtering messages based on size* starting on page 6-2.
- The **Disclaimer Manager** allows you to append disclaimers within messages. For more information, see *Adding a disclaimer to messages* starting on page 6-4.

Heuristic spam filter

For complete information on using the heuristic spam filter, see *Filtering Content with the Spam Prevention Solution Filter (SPS)* on page 7-1.

Creating sub-policies

A sub-policy contains one or more user-defined filters. A policy-creation wizard guides you through the process.

Note: Including the **Global Policy**, a sub-policy can have a depth of up to five sub-policies. A maximum of 10 sub-policies can be created within a single policy. However, each sub-policy can have an unlimited number of filters.

The main steps are detailed below:

1. Create the policy
2. Define the route
3. Add a user-defined filter
4. Choose filter actions
5. Add additional filters

Step 1: Create the policy

To create a policy:

a. In the navigation panel, click **Policy Manager** > **Global Policy** > ***Policy Name***.

b. Click the **Sub-policies** link at the top of the screen.

c. Under the **Sub-policies** link, click the **Create new sub-policy** link.

d. Enter a name and description for the sub-policy and click **Next**.

To change the name of the sub-policy you just created, click the **Settings** link.

To determine the order in which the sub-policies are listed:

1. Click the **Sub-policies** link and the **Manage sub-policies** screen is displayed.
2. In this screen, highlight a sub-policy and click the **up** or **down** arrows.
3. Click **Save**.

Predefined sub-policies

By default, the InterScan MSS installation program creates the following sub-policies, based on the domain name that you entered in the installation wizard:

- **Incoming**
- **Outgoing**
- **POP3 message**

The **Incoming** and **Outgoing** policies enable virus checking on all messages that pass through the InterScan MSS server and provides a basis for applying additional policies.

The **Incoming Policy** has the following policy condition:

- Messages from * going to **@domain*

The **Outgoing Policy** has the following policy condition:

- Messages from **@domain* going to *

Both of these policies contain an active **Antivirus Filter**, which has the following configurations:

- All attachments are scanned, including compressed files
- Viruses are cleaned, and uncleanable viruses are deleted
- When a virus is cleaned, a disclaimer is added to the message before it is delivered
- If a virus cannot be cleaned, or scanning is halted, the message is quarantined and a notification is sent
- Any mass-mailing virus is deleted

The **Incoming Policy** also contains some content management policies that restrict message size, for attachments that can potentially harbor viruses, and for multimedia file attachments. These filters are disabled, but you can customize and enable them.

The **Outgoing Policy** contains an inactive **Message Size Filter** that you can activate and configure.

By default, InterScan MSS provides a new policy, called the **POP3 message policy**. If you accidentally delete this sub-policy, you can create another one during the match policy process by applying a unique route for POP3 messages. As a result, the POP3 message is matched only to the policy with this unique route.

InterScan MSS matches all POP3 messages to the **POP3 messages policy**. If you do not create this POP3-only policy, the POP3 message is matched to the global policy. For additional information on POP3 mail scanning, see *Scanning POP3 messages* starting on page 3-13.

If you are modifying the route information of this POP3-only policy, make the same modifications to the .ini file. Any modifications you make to the route have to be in the name part of the route (before the @). Modifications to the .ini file have to be only to the name part of the route without the @ or other illegal characters. If these conditions are not met, the policy will not work.

Policy and address matching

When InterScan MSS receives a message for processing, it executes the best match policy whose route matches the sender/receiver addresses. If an exact match is found, InterScan MSS stops searching and performs the filter action associated with that policy. If an exact match cannot be found, it continues until a best match is found. For additional information on how the best match is calculated, see *Priority rules* starting on page A-7.

For example, suppose your installation has two sub-policies, Policy A and Policy B with the following incoming routes:

- Policy A's route: * to *@company.com
- Policy B's route: * to raymond@company.com

If the recipient is raymond@company.com, InterScan MSS performs Policy B's filter action, because an exact match has been found.

Step 2: Define the route

What is a route?

A route is a subset of messages being processed by your InterScan MSS server. When you create a new policy, the route is determined by the email addresses you enter in the fields under the **From** and **To** columns. In other words, the route is the sub-policy's scope.

Using the "*" Wildcard In Routes

- Single * Wildcard

  A single * wildcard matches everything, including nothing. For example, if you enter a single *, it matches all of the following:

  - stanley@trendmicro.com
  - nothing (some spam messages have empty **From:** fields when the sender does not want to disclose his identity)

- Using * in an expression

  The behavior of wildcard * differs whether it appears before or after the @ in an email address. Text that comes before the @ is treated as the name portion of the address; text that comes after @ is treated as the domain portion. If no @ exists, then the entire string is considered invalid. For example, strings such as "abc" or "trendmicro.com" are invalid.

- Name Pattern

  To match the name portion, you can only use a single wildcard * or the exact name. Partial matches are not allowed. The wildcard matches everything except no entry in the field.

  For example:

  - *@trendmicro.com matches stanley_edwards@trendmicro.com
  - *@trendmicro.com does not match @trendmicro.com
  - Joe*@trendmicro.com or *edwards@trendmicro.com is not allowed

- Domain Pattern

  For the domain portion of the address, the wildcard * can only occur at the beginning of the pattern, and it can match one or more subdomains.

  For example:

- *@*.solar.com matches *@earth.solar.com
- *@*.solar.com matches *@europe.earth.solar.com
- *@*.solar.com does not match *@solar.com
- *@*.*.com matches *@earth.solar.com

Partial matching of subdomains is not allowed. For example, *@trend*.com is an invalid format.

Other incorrect patterns are:

- *@trend.*.jp (wildcard occurs in the middle of the domain name)
- *@trend.com.* (wildcard occurs at the end of the domain name)
- *@*.*.com (second wildcard occurs in the middle of the domain name)

Defining the route

To define the route:

1. Click the **Route** tab at the top of the policy screen.
2. In the fields under the **To** and **From** columns, enter the email address of the message set for which the sub-policy will apply.

Note: For a sub-policy, the email addresses you enter for the route must be a subset of the parent policy. For example, the address you enter for an **Incoming Policy** must be a subset of the email addresses you entered for the **Global Policy**.

---

3. Click the **Select** link to use an existing address group.
   Address groups are an efficient way to manage route definitions and ensure that a consistent policy is applied to different departments. For more information, see *Managing address groups* starting on page 4-4.
4. Click **Save**.

Step 3: Add a user-defined filter

Click the **Filters** link to see the **Manage filters** screen and the following links:

- **Order filters**
- **Create new filter**

In the **Manager filters** screen is the **Filters List**, which shows the filters that the sub-policy inherited from its parent (for example, the **Global Policy**) and the status of each of these filters.

Note: A policy can only contain one antivirus filter. If both the parent and sub-policy have an **Antivirus Filter**, the filter in the sub-policy is executed.

Creating a new filter

To create a filter:

1. Click the **Filters** link then the **Create new filter** link.
2. Enter a name for the filter and specify whether this filter can be overwritten by another filter in a sub-policy.
3. Select a filter from the **eManager Filter group** and click **Next**.

Now, the sub-policy creation wizard displays screens that are appropriate for the filter that you have chosen to add. For more information about configuration options for each type of filter, see *Understanding the available filters* starting on page 4-19.

Step 4: Choose filter actions

For each filter result, select a filter action.

Note: The filter actions must be defined before you create the filter. For more information on filter actions, see *Managing filter actions* starting on page 4-10.

The **Antivirus Filter** options are:

- Messages with potentially malicious compressed attachments (IntelliTrap)
- Mass mailing virus detected
- Virus or spyware/grayware detected but some/all were not cleaned or deleted
- Joke program attachment detected
- Virus(es) detected and successfully cleaned
- Virus scanning aborted—message may contain viruses
- Password-protected file detected (not scanned)
- Virus or spyware/grayware detected and successfully cleaned or deleted
- Virus(es) detected but some/all were not cleaned
- No virus detected

For filters using the eManager filter, there are only two results:

- Triggered (matches filter settings)
- Not triggered

For filters using the SPS heuristic filter, there are only two results:

- Triggered (identified as spam)
- Not triggered

Step 5: Add additional filters to the sub-policy

A sub-policy can contain multiple filters. After adding the first filter, choose the additional filters that you want to apply to all the messages in the route that you have defined.

When you have finished adding filters to your sub-policy, you are returned to the **Filter List** window, which displays all of the filters that you have added.

Order of filter execution

The order of execution of filters in a sub-policy is significant because, if a message is being processed and a **Delete** action is triggered, the message is deleted and filter execution stops.

To determine the order of a sub-policy's filters:

1. Click **Policy Manager** > **Global Policy** > ***Your Policy***.
2. In the **{Policy Name}** screen, click the **Filters** link > **Order filters** link.
3. The **Order filters** screen shows the order that filters in the sub-policy are executed. To change the order of execution, highlight a filter in the list and click the **up** or **down** arrows. Multiple-selection is allowed.
4. When the filters are arranged in the preferred order, click **Save**.

Execute the antivirus filter first

If your sub-policy contains an **Antivirus Filter**, we strongly recommend that you put it at the top of the **Order filter** list so that it executes first. This step prevents a virus-infected message from being quarantined and later delivered without being scanned.

If you have a filter that has its action set to delete, you may safely place that filter before the **Antivirus Filter**, since there would be no danger of the filter quarantining an infected message. This has the benefit of improving system performance, since fewer messages will require antivirus scanning or processing by other filters.

Chapter 5

Using the Antivirus Filter

This chapter explains how to use the **Antivirus Filter** in your policies.

Topics include:

- Selecting which message attachments should be scanned for viruses
- Choosing a filter action
- Deleting viruses and inserting disclaimers
- Managing the following:
  - Mass-mailing viruses
  - Joke programs
  - Password-protected files
- Testing the virus scanning engine

Selecting message attachments to scan

To configure the default Antivirus Filter in the Global Policy:

1. In the navigation panel, click **Policy Manager** > **Global Policy**.
2. Click **Edit** in the Virus Filter **Filter Type** column.

The **File Types to Scan** screen is divided into the following parts:

Selecting File Types to Scan

- **Scan all file types**:

  This option is the safest but most resource-intensive; if this option is selected, InterScan™ MSS scans every attachment.

- **IntelliScan**:

  Optimizes performance by examining file headers using true file type recognition, and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by using a harmless file extension type.

- **Scan specified file types by extension**:

  This setting scans files by extension, not by true file type. More comprehensive protection is offered by true file type identification using **IntelliScan** or the **Scan all file types** option.

  When you select this option, the **Edit** button is activated. If you click **Edit,** the **Edit Specified File Types** screen is displayed and is divided into the following sections:

  - **Default extensions**
  - **Additional Extensions**
  - **Extensions to Exclude**

  To add multiple file extensions, type a semi-colon (;) between each entry.

Scanning compressed files

Compressed archives such as *.zip, *.arj, *.lzh, etc. are the preferred method of transferring large files through messaging systems and using HTTP/FTP downloads. Compressed files can harbor viruses. However, since the archive has to be

decompressed, scanning these files is resource intensive. This issue is particularly acute when a compressed file is made up of other compressed files.

If you select the **IntelliScan** option, by default, compressed files are scanned. For more information on **IntelliScan**, see *Selecting File Types to Scan* starting on page 5-2. Click **Cancel** or **Save** to return to the previous screen.

Using wildcards

You can use the "*" and "?" wildcard characters when configuring **File Types to Scan** and **File Types to Exclude**. The "*" represents any number of characters, but the "?" represents a single character.

Usage examples include:

- Typing "*" scans all files, regardless of the extension
- Typing "do?" scans files with a three-character extension that starts with "do", such as .dot and .doc
- Typing "e*" scans all files with extensions that start with "e" regardless of the extension length

Excluding file types from scanning

The behavior is similar to wildcard usage. If you enter a "*" it means that only files without extensions are scanned.

Setting Virus Actions

When the scan engine detects a virus, it can be configured to take one of the following actions against the message attachment:

- **Clean**, where the virus code is removed from the file

  Some viruses and file types cannot be cleaned; if you choose **Clean**, also choose a follow-up action using the pull-down menu
- **Delete**, where the file is permanently deleted and cannot be retrieved
- **Pass**, where no action taken

Configuring IntelliTrap

Virus writers often attempt to circumvent virus filtering by using different file compression schemes. Trend Micro IntelliTrap provides heuristic evaluation of compressed files that helps reduce the risk that a virus compressed using these methods will enter your network via email.

Because there is the possibility that IntelliTrap may incorrectly identify a non-threat file as dangerous, Trend Micro recommends quarantining message attachments that fall into this category when the IntelliTrap feature is enabled. In addition, if your users regularly exchange compressed files, you may want to disable this feature.

To configure IntelliTrap:

1. Select **Enable IntelliTrap**.
2. Choose a **File Action**:
   - Choose **Delete** to delete any attachments that IntelliTrap detects as potentially malicious
   - Choose **Pass** to allow the attachment to be delivered and only write a detection entry in the InterScan™ Messaging Security Suite logs
3. Select **Also send a sample to TrendLabs** to send only the attachment to TrendLabs. This allows Trend Micro to collect data about files that are detected by IntelliTrap and improve this feature.

Notifying recipients

InterScan MSS can add disclaimer text to messages when a virus is found. Type your disclaimer text in the text box under this option. A **safe stamp** can be added to messages and attachments that are found to be virus free.

Choosing a filter action

To configure the filter action in the Global Policy's default Virus Filter:

1. In the navigation panel, click **Policy Manager** > **Global Policy**.
2. Click **Edit** under the **Virus Filter**'s **Action** column.

For each result, configure a filter action. See *Using filter actions* starting on page 4-7 for more information.

The **Virus Filter** has the following possible filter results:

- Messages with potentially malicious compressed attachments (IntelliTrap)
- Mass mailing virus detected
- Virus or spyware/grayware detected but some/all were not cleaned or deleted
- Joke program attachment detected
- Virus scanning aborted—message may contain viruses
- Password-protected file detected (not scanned)
- Virus(es) detected and successfully cleaned
- No virus detected

Note: Since the scan engine cannot open encrypted messages, it cannot analyze them. Encrypted messages are processed based on your exception handling configuration.

Examples

To help understand how the filter actions work, here are two examples:

1. A single message with the following four types of attachments:
   - Password-protected file
   - Cleanable attachment
   - Non-cleanable mass-mailer attachment
   - Joke

   In this example, regardless of whether the virus can (or cannot) be cleaned, the outcome is mass mailer, because it has the highest priority.
2. If a single message has the following combination of attachments:
   - Password-protected file
   - Cleanable attachment
   - Joke

   The outcome in this example is Joke, because Jokes have the highest priority.

Using ActiveAction

All of the preconfigured filter results are based on ActiveAction, which is a set of scan actions to be performed on viruses and other types of malware.

ActiveAction identifies virus types and recommends actions based on how each type invades a computer system or environment. ActiveAction categorizes viruses by malicious code, replication, and payload types. When the **Antivirus Filter** in InterScan MSS detects a virus, the recommended action for the virus category is taken to protect your environment's vulnerable points.

The recommended action for viruses is **Clean**, for Trojans and joke programs is **Quarantine**, and for test viruses is **Bypass**.

Choosing an action for uncleanable files

Some application files, which can potentially harbor viruses or malicious content can be password-protected. Since files have to be opened to be scanned, this could be a way for malicious content to enter your messaging system.

When InterScan MSS receives an unscannable message, although it cannot be scanned, the filter action you set is performed. For more information, see *Using filter actions* starting on page 4-7.

Understanding the execution order of filter actions

When a file is received by InterScan MSS, the **Virus Filter** determines whether the file can (or cannot) be scanned. If it is deemed unscannable, the filter action you set for password-protected or other unscannable files is performed. If it can be scanned, the filter will determine whether it is a mass mailer, a joke, or other and take the appropriate action that you selected.

Processing messages sent to multiple recipients

If a virus-infected message is sent to multiple recipients in different domains, InterScan MSS may show a record of processing one message, but virus detection is shown for each recipient.

Testing virus detection

The European Institute of Computer Antivirus Research (EICAR) and some antivirus vendors have developed a test file that you can use to check if your system detects viruses.

The file is not a virus, so it causes no harm and does not replicate. It is a specially-created file whose “signature” has been included in the Trend Micro virus pattern and can be detected by the Trend Micro scan engine.

To download this file from the Trend Micro Web site, go to:

`www.trendmicro.com/en/security/test/overview.htm`

You may need to disable HTTP scanning before you download the file. To test SMTP scanning, include the test virus as an email attachment.

You can also copy the following text into a text file and save it with a “.com” extension (for example, virus.com):

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Chapter 6

Filtering Content with the eManager™ Filtering Tools

This chapter explains how to use the eManager filter tools to manage message content, enforce email usage policies, and reduce the amount of spam that passes through your messaging system.

Topics include:

- Working with the eManager filters
- Filtering messages for keywords
- Expressions that evaluate sample content
- A case study that illustrates the filtering of prohibited keywords for innocent usage
- The evaluation order of expressions
- The seven types of valid expressions
- Using reserved words in your keyword expressions
- Handling MIME subtypes
- Writing file extensions in expressions

Working with eManager filters

The eManager filters provide powerful tools for managing message content. These filters allow you to control the delivery of large messages to improve network performance, add disclaimers to messages, and perform other filter actions on messages based on keyword expressions.

The eManager filter also filters the contents of files attached to a message in a zipped archive (`.zip` files). Filename filter settings and true file type checking settings apply to files inside a compressed attachment for the Attachment filter.

Note: These filter settings for archive files work on the first twenty levels of recursive compression for true file type scanning, and for the first level of compression for filename scanning.

Filtering messages based on size

The **Message Size Filter** allows precise control over the types of messages that can be processed at different times of the day. You can use it to postpone processing large messages until non-peak hours, such as nights and weekends.

Features

- Supports message filtering based on:
  - Message size (body + attachments)
  - Attachment size
  - Number of attachments
- Message size restrictions are enforced during one-hour intervals selected from the activation schedule (Figure 6-1).

Creating or modifying the filter

To create or modify a Message Size Filter:

1. Choose the size of the message parts that you want to filter by selecting one of the options (see *Features* starting on page 6-10).
2. Click **Activation Schedule**. Select the time slots during which messages that exceed the size limits trigger the filter.

   As you can see in Figure 6-1, the default times when messages that trigger the filter are blocked at the SMTP gateway are Monday through Friday from 7:00 AM to 6:00 PM.

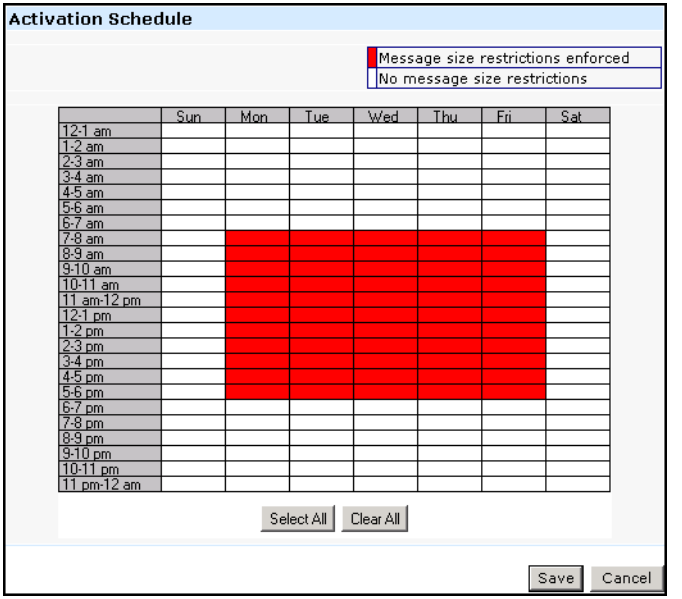


FIGURE 6-1. Message size filter—activation schedule

3. Click **Save**. You are returned to the **Filtering criteria** screen.

Adding a disclaimer to messages

The **Disclaimer Manager** allows you to add standard text in messages that you specify.

Features

- Adds user-configurable disclaimer text at the beginning or end of messages
- Supports complex expressions using the eManager filters
- Also adds a disclaimer to all messages (those that match and do not match) the expression

Creating or modifying the filter

To create or modify the Disclaimer Manager Filter:

1. Under Step 4-1, type the contents of the disclaimer.
2. Choose whether the disclaimer will be appended at the beginning or at the end of the message body.
3. Select the messages to which the disclaimer applies:
   - **All messages**
   - **Messages that trigger at least one of the filter's expressions**
   - **Messages that do not trigger any of the filter's expressions**
4. If you chose to insert the disclaimer based on an expression, click **New Expression** under Step 4-3 and configure it. For more information about configuring expressions using the eManager filter's built-in operators, see *Using complex expression syntax* starting on page 6-17.
5. Click **Next**.
6. Verify your settings and click **Next**.

   Clicking **Next** saves your settings, so you cannot return to previous screens in the wizard.
7. Using the pull-down menus, select the filter action and click **Save**.

Filtering messages for keywords

The **Advanced Content Filter** allows you to filter all parts of a message for simple or complex expressions. You can also check for keyword synonyms using the built-in synonym list. Several of the default content filters, such as **Profanity**, **Racial Discrimination**, **Sexual Discrimination**, **Hoaxes**, **Chainmail**, and **Block HTML Script Messages** are **Advanced Content Filters**.

To see an example of this filter, in the navigation panel, click **Policy Manager** > **Global Policy** and click **Edit** next to any of the default filters that use the **Advanced Content Filter**.

Features

The **Advanced Content Filter** provides the following functionality:

- Filters content in:
  - **Mail header** (**Subject**, **From**, **To**, **CC**, or any other header field)
  - **Mail body**
  - **Mail attachment**

    You can scan messages by content or file name. Also, when the severity index exceeds the threshold, you can choose to strip the attachment from the message.

    Text, HTML, Microsoft™ Excel™, Microsoft™ PowerPoint™, and rich-text format (rtf) attachments can be scanned.
  - Configurable severity index permits the configuration of a filter's sensitivity to keyword matches.
  - eManager's built-in operators that support the following complex expressions:
    - Keyword expression case sensitivity
    - Optional keyword synonym matching

In addition to this functionality, it is important to consider keyword frequency and proximity when deciding to trigger the filter.

Filtering different parts of a message

eManager can filter the following messages sections:

- Mail header: You can choose to filter the message **Subject**, **From**, **To** or **CC** fields. The **Other** option allows you to filter another field that commonly appears in a message header such as **Received, Message-ID**, **Date**, **Reply-To**, **Sender**, and so on.

Note: When entering the field name, do not enter the colon ":" character that usually follows a field name in a message header. The **Other** field can only be used to specify one user-defined message header field.

- Mail body: The visible text in the message and any HTML tags.
- Mail attachment: You can filter both the content and file names of message attachments. The eManager filter can check content in .txt, HTML, Word, Excel, PowerPoint, and .rtf files.

In addition to the **Advanced Content Filter**, there are five other predefined eManager filters that you can use in your policies. These are available when you create a new filter.

When the mail header (**From**, **To**, and **cc**) and the body of the mail are scanned, separators, quotation marks (“), a comma (,), brackets (<>), and a semicolon (;) are added. These separators are not removed when you clear the filter's mail header.

If the **severity index** scanning result exceeds the threshold, you can automatically delete the attachment before sending it to the final recipient. For more information, see *Intelligent keyword matching* on page 6-9.

Filtering Messages Based on Expressions

The **Advanced Content Filter** searches for keyword expressions that you define.

The expressions that a filter contains are shown in the **Expression** list.

To enter a new expression:

1. In the first page of the **Advanced Content Filter** that you are creating or modifying, click **New Expression**.
2. In **Expression**, type the expression to filter. For more information about writing complex expressions using the eManager filter's built-in operators, see *Using complex expression syntax* starting on page 6-17.
3. If you want incidences of your keywords to be filtered (regardless of their case), under **Case sensitive**, select **Disable**.
4. The eManager filters include a synonym dictionary that allows you to enable the synonym filtering of your entered keywords. To do this, select **Detect synonyms** and click **Edit**.
5. The **Available Synonyms** panes show the synonyms for the keywords that you have entered in your expression. To move them to the **Detect these Synonyms** pane, select them and then click >>; to move them back to the left pane, select them and click <<.

   Ctrl-clicking allows you to select a non-contiguous range; shift-clicking allows you to select a continuous range.
6. When the right panes show the synonyms that you want to detect, click **Done**.

To access the **Advanced Settings** screen, click **Advanced Settings** in the main **Advanced Content Filter** screen.

Proximity

Proximity is significant because the keywords that you want to filter only constitute prohibited content when they appear close to each other. Consider the following message samples—the first one is taken from a church newsletter:

> ...picnic was a tremendous success. All of the children were treated to fruit **punch** and cookies. Following snack time, they played games until the clown showed up to distribute presents, with children laughing at his painted **face** and colorful clothes...

This second example came from a hot-headed colleague:

> ...be forewarned, if your bill collectors persist in calling me, I will come down to your office and **punch** your **face** into oblivion...

The relational operator .NEAR. allows you to take the proximity of keywords into consideration. In an expression such as

```
punch .NEAR. face,
```

the **Proximity** value is 2. This expression triggers on the colleague's message but not on the church newsletter.

The proximity is calculated in the following fashion, where 3 - 1 = 2:

punch	your	face
1	2	3

Table 6-1. Calculating Proximity Values for the .NEAR. Operator

If you write an expression that uses the .NEAR. operator, remember to enter a value in the **Proximity** field. For more information about the .NEAR. operator, see *Relational operator* starting on page 6-24.

Frequency

The frequency of keyword expressions is also configurable. You may want your filter to trigger, for example, only if a certain keyword expression appears several times. This step provides a few chances for your users to use the prohibited keywords, but the filter is still triggered if these words are excessively used.

The limiting operator .OCCUR. can be used to consider the frequency of a keyword expression. For example, consider a filter that contains the expression:

```
.OCCUR. free
```

If the **Frequency** value is set to 5, it means that this filter triggers if “free” appears in the content sample five or more times.

Separators

By default, the eManager filter “tokenizes” (divides or parses into words), message content by using the space, tab, line feed and return characters. Content between these characters is considered to be separate tokens and is compared to your keyword expressions. If you want other characters to be used to tokenize keywords, enter them in the **Separators** field.

Intelligent keyword matching

You can assign **Advanced Content Filter** expressions a severity value. Each time the expression is detected, its value is added to a total. The filter is triggered when this total exceeds the severity threshold.

To consider severity during keyword expression filtering:

1. Select **Enable intelligent keyword matching**.
2. In the **Severity threshold** field, enter the severity threshold that will trigger the filter.
3. Click **Edit**.
4. Assign a severity value between 1 and 10 for each keyword expression.
5. Click **Done**.

Can you assign negative severity?

No - severity values can only be positive. But if you want to ignore a keyword when it occurs in conjunction with another term, you can configure this kind of filter behavior by using the .AND., .OR. and .NOT. operators (see *Complex expression example* starting on page 6-25).

How severity is calculated

When calculating severity, each message "entity" (header, body and attachment) is considered separately. For example, suppose you set the severity threshold to 10, and set two keywords (A and B) each with a weight value of 5. A message with a subject that contains A and mail body that contains B does not trigger the filter because they are found in different entities.

Filtering message attachments

Attachment filter type blocking stops message attachments or MIME content-types at the SMTP gateway.

Features

- Checks messages by attachment:
  - Name (supports wildcard usage)
  - Types from MIME content-type field in the message header
  - File type from a binary analysis of the attachment
- Optionally allows automatic deletion when a filter is triggered.

Creating or modifying the filter

To modify a filter or create a new one, first follow the instructions below. To create a new filter:

1. From any policy screen, click the **Create new filter** link.
2. In the **New Filter** screen, complete steps 1-3 and click **Next** >>. You are returned to the **Manage Filters** screen for your policy.
3. Go to the appropriate filter section in this chapter for more detailed information.

To modify a filter:

1. Go to the policy screen to which the filter applies.
2. To modify the filter's parameters, click **Edit** next to the filter under one of the following columns:
   - **Filter Type**
   - **Filter Availability and Status**

- **Filter Action**

3. See the steps in the following section for more detailed information.

Next, proceed to the detailed instructions under each filter section.

Creating or modifying the filter

To create or modify a Message Attachment Filter:

1. Select which of the following attachment types you want to filter.
   - **Attachment file extension and/or name**:

     Enter a complete file name (readme.exe) or a wildcard expression (*.mp3).
   - **Message MIME content-type**:

     To select specific MIME content-types, click **Edit**. In the **MIME content-type** screen, select the file types and click **Done**. For additional information, on the MIME content-type, see *Message MIME content-type* starting on page 6-12.
   - **Attachment file type**:

     To select a specific attachment file type, click **Edit**. In the **Attachment file type** screen, select the file type(s) and click **Done**.

Will changing the attachment's file extension avoid attachment blocking?
No. The eManager filter does not rely on a file's extension to determine the file type, but instead performs an internal analysis of the file.

2. Select **Option** if you want the attachment to be stripped and discarded when the filters' conditions are triggered.
3. Click **Next**.
4. In this screen, verify your settings by clicking **Next** again. Clicking **Next** saves your settings, so you cannot return to previous screens in the wizard.
5. Using the pull-down menus, select filter actions and click **Save**. You are returned to the policy screen to see your newly created filter in the list.

Note: When choosing to block messages by attachment file type, Java byte code refers to Java class files with the `.JS`, `.JSE`, `.CLA`, and `.CLASS` extensions.

Some file types in this screen include several subtypes.

Under **Executable**:

- **exe** includes all DOS, Windows 3.1, 32-bit Windows and OS/2 executable files
- **dll** includes both Windows 3.1 and 32-bit Windows DLLs

Under **Compressed Files**, the **others** option includes the LZW, CAB, LHA, ARC, AR, PKLITE, DIET, LZH and LZ compressed file formats.

Message MIME content-type

In the main **Message Attachment** screen you can also choose to scan MIME content-types. Email messages with MIME content contain a **Content-Type** field in their header.

The following shows a sample email message header:

```
Mime-Version: 1.0
Content-Type: multipart/mixed;
This is a multi-part message in MIME format.
Content-Type: text/plain; format=flowed
Content-Type: application/msword;
...
```

The **Message Attachment Filter** can detect these MIME types and perform the action that you configure.

The following is a mapping table that shows how the eManager filter blocks certain MIME content-type attachments. You can use this table to determine which MIME content-type is blocked by enabling the corresponding item in the screen. Click **Done** when you have finished

.

UI Wording	MIME content-type(s)
Image file formats	
jpeg	image/jpeg, image/pjpeg
gif	image/gif
tif/tiff	image/tiff
bmp	image/x-ms-bmp, image/bmp
Audio file formats	
wav	audio/x-wav, audio/wav, audio/microsoft-wave
mp3	audio/x-mpeg, audio/mpeg
midi	x-music/x-midi, audio/mid
Video file formats	
mpeg	video/mpeg
quicktime	video/quicktime
msvideo	video/x-msvideo, video/avi, video/x-ms-asf, video/x-ms-wmv
Application file formats	
pdf	application/pdf
zip	application/zip, application/x-zip-compressed
msword/rtf	application/msword, application/rtf, text/richtext
mspowerpoint	application/vnd.ms-powerpoint, application/ms-powerpoint
msexcel	application/vnd.ms-excel, application/x-msexcel, application/ms-excel

Table 6-2. MIME Content-type Blocking Filter

Note: The exact wording in the message's **Content-Type** field differs slightly depending on which email client sends the message. To see the terminology used by some common email clients, see *MIME Content-types used by email clients* in Appendix A, starting on Page A-9.

Filtering content using the general content filter

The **General Content Filter** is a simple content and attachment filter that lets you filter by the:

- **Subject line** (permits multiple subjects)
- **Keyword(s)** in the message body
- **Attachment file size**
- **Attachment file extension** (supports wildcard usage)

Features

This filter also supports case sensitivity.

The **General Content Filter** cannot use complex expressions that include the built-in operators .NOT., .OCCUR., and so on. If these terms are entered, they are treated as part of the keyword expression, not as an operator.

Note: When configuring the **General Content Filter**, enter a **Subject line**, **Mail body** or **Attachment file name** expression that includes the wildcard "*". However, the expression cannot consist entirely of a "*"

Creating or Modifying the Filter

To create or modify a General Content Filter:

1. Choose from the following criteria to trigger the filter:
   - **Subject line is**

     This option supports wildcard "*" usage in an expression.
   - **Mail body contains**

     This option supports wildcard "*" usage in an expression. You can use the pull-down menu to select whether you want **All keywords**, **Any keywords**, or **No keywords**.
   - **Message size is**

     This option allows you to filter attachments that are larger or smaller than the settings that you entered.

- **Attachment file name contains**

  This option supports wildcard "*" usage in an expression.

2. Click **Next**.
3. Verify the filter settings you selected and click **Next**.

   Clicking **Next** saves your settings. You cannot return to previous screens in the wizard.
4. Using the pull-down menu, select a filter action and click **Save**. You are returned to the policy screen to see your newly-created filter in the list.

Writing expressions for eManager content filters

Message content is compared to keyword expressions and other criteria that you configure in the filters. Messages are processed based on the following:

- The filter's mail evaluation result
- User-configured filter actions

To search for keywords more efficiently, you can use regular or complex keyword syntax.

Separating keywords in dialog boxes

Most of the eManager filters allow you to delimit multiple keywords with a semi-colon (;). But what happens if you want to search for a keyword expression that includes a colon, for example, *I like not only dogs; but also cats*?
To search for keyword expressions that contain a colon, you must precede the colon with a backslash. The keyword expression above could be searched by typing *I like not only dogs\; but also cats*.

Using regular expression syntax

Note: Regular expressions can only be used in the **Advanced Content Filter**, because only this filter accepts operators.

The regular expression feature in InterScan MSS supports matches within a word, but not across words. For example, **a.*e** matches **advance**, but not **achievement made**. To specify a regular expression, add a **.REG.** operator before that pattern (for example, **.REG. a.*e**).

Tip: Do not use \n, \r, or \t as regular expressions, because they are InterScan eManager separators.

The table below provides the details on using this expression:

Character	Description	Example
.	This wildcard matches any character, except a new-line character.	An expression like **a.c** matches any character between **a** and **c**; but, **ab** (first line) and **c** (new line) is not a match.
?	This wildcard matches zero or one instance of the preceding regular expression.	An expression like **a?c** means that the character **a** can be zero or one, so it can match characters such as **c** or **ac.**
*****	This wildcard matches zero or more of the characters in the preceding regular expression.	An expression like **P*K** matches characters such as **K**, **PK, PPK, PPPPK.**
+	This wildcard matches one or more instance of the preceding regular expression.	An expression like **P+K** matches characters such as **PK, PPK, PPPPK.**
[abc]	This syntax matches any one of the enclosed characters.	An expression like **b[ave]d** matches characters such as **bad, bvd, bed**

Character	Description	Example
[a-c]	This syntax matches any one of the enclosed range of characters; but, the character in this syntax can be only letters and numbers (for example, [a-c], [A-E], [0-9]). Specifying any other range is unsafe and is not allowed.	An expression like **b[a-c]d** matches characters such as **bad, bbd, bcd.**
[^a-b]	This syntax matches any character that is not in the specified range.	An expression like **[^a-z]** matches characters such as **1**, **H**, **K**, but not **f**, **g**, **j**.
{n, m}	This syntax matches a range of occurrences of the character that precedes it; The preceding character can also be a regular expression. For example, **{n}** matches at least “n” occurrences, and **{n,m}** matches any number between “n” and “m”.	**An expression like 0 {5}** matches characters such as five zeroes in a row.

The backslash character “\” is used as the escape character. The first and last character of the regular expression should match the boundary of a token; no substring match is allowed. You can perform case-sensitive matches, and the expression is evaluated from left to right.

More complex examples include:

- B.*V, which matches BV, BAV, BFFFV, B1232V, and so on
- B[*\+]V, which matches B*V and B+V.
- [AB][123]?, which matches A1, B, B3, and so on

Using complex expression syntax

A legal keyword expression is composed of tokens, which is the smallest unit used to match the expression to the content. A legal token can be an operator, a logical symbol, or the operand, i.e., the argument or the value on which the operator acts. Legal operators include .AND., .OR., .NOT., .NEAR., .OCCUR., .WILD., “.(.” and “ .).” The operand and the operator must be separated by a space. An operand may also contain several tokens.

Using separator characters

The eManager filter uses several characters to parse the keyword expression into tokens. Words between these characters (known as separators), become a token.

The eManager filters uses the following separators to tokenize keyword expressions:

Character	Space
	space
\t	tab
\n	linefeed
\r	carriage return

Table 6-3. Separators for tokenizing expressions

Note: A space between the operand and the operator is significant to how the expression is tokenized. For example, the expression “High .AND. Low” is tokenized as two operands (“High”, “Low”) and one operator “.AND.”. The expression “High.AND.Low” is tokenized as one operand (“High.AND.Low”).

Using operators

The operators used by the eManager filter can be categorized into five groups. All operators are reserved words and cannot be used as a keyword token to match content.

Category	Operators	Functionality
Grouping operator	.(. and .).	Used to change the evaluation order. The expression within these operators is evaluated first.
Decorating operator	.WILD.	Will match if the content contains the operand. Wildcard character (*) can be used as an operand of .WILD.
Logical operator	.AND., .OR., .NOT.	Performs specific logical operations on operands

Category	Operators	Functionality
Limiting operator	.OCCUR.	If the number of occurrences of the operand is greater than the preset number, this condition will be triggered.
Relational operator	.NEAR.	If the token count between the last token of the first operand and the last token of the second operand is less than the preset number, the condition is triggered.

Table 6-4. Operator Categories

Priority of operators

When evaluating an expression, the following priority levels are used (1 is the highest and 5 is the lowest):

Operator	Priority
.(.	*
.).	*
.WILD.	1
.OCCUR.	2
.NOT.	2
.NEAR.	3
.AND.	4
.OR.	5

Table 6-5. Operator priority

Expression examples

The following examples show expressions that use the operators and how these operators evaluate when sample text is tested.

Grouping operators

better .AND. faster .OR. cheaper

This expression matches content that contains “better” and “faster” It also matches content that contains “cheaper”.

Content	Result
...analysts agree that the 2004 model is a **better**, **faster** and more economical vehicle than its predecessors...	Match
...many young families have found that buying houses in the East Bay suburbs is **cheaper** than living in the Peninsula communities...	Match
...broadband Internet access can be up to 50 times **faster** than dial-up connections, and rates are expected to...	No match

Table 6-6. Grouping operator [*better .AND. faster .OR. cheaper*]

better .AND. .(. faster .OR. cheaper .).

This expression matches content that contains “better” and any instances of “faster” or “cheaper.

Content	Result
...analysts agree that the 2004 model is a **better**, **faster** and more economical vehicle than its predecessors...	Match
...many young families have found that buying houses in the suburbs is **cheaper** and offers a **better** quality of life...	Match
...broadband Internet access can be up to 50 times **faster** than dial-up connections, and **cheaper** rates are on the...	No match

Table 6-7. Grouping operator [*better .AND. .(. faster .OR. cheaper .).*]

Decorating operator (.WILD.)

.WILD. This * message

This expression matches content when “message” follows “This”. There can be any number of words between “This” and “message”.

Content	Result
...**This message** is being sent to you because you signed up for our free email newsletter...	Match
...**This** is to inform you that I will be on holidays until 10/12. You can leave a **message** at 408-555-1212...	Match
...**This** is arguably the most exciting software that I have...	No match

Table 6-8. Decorating operator [*.WILD. This * message*]

.WILD. *ed

This expression matches any content that ends with “ed”.

Content	Result
...that movie has been edit**ed** for TV broadcast...	Match
...this program is follow**ed** by an infomercial...	Match
...The **ed**itor sent the manuscript for final proofreading...	No match

Table 6-9. Decorating operator [*.WILD. *ed*]

Logical operator (.AND., .OR., .NOT.)

High .AND. Low

This expression matches content when “High” and “Low” are present.

Content	Result
...**High** today in the interior is 87. **Low** tonight will be 53 near the coast...	Match
...His favorite movies are “**High** Noon” and “Eject at **Low** Level and Live”...	Match
...she plans to attend Central **High** next fall...	No match

Table 6-10. Logical Operator [*High .AND. Low*]

High .OR. Low

This expression matches content when “High” or “Low” are present (also matches content when both words are present).

Content	Result
...**High** tide will be at 9:00 PM. **Low** tide will be at 7:00 AM...	Match
...she’s planning to move to **High** Street in July...	Match
...please turn the heater to **Low** - I’m sweating...	Match

Table 6-11. Logical operator [*High .OR. Low*]

.NOT. Happy

This expression matches content when “Happy” is not present.

Content	Result
...**Happy** Birthday to you...	No match
...**Happy** Hanukkah...	No match
...Merry Christmas...	Match

Table 6-12. Logical operator [*.NOT. Happy*]

How expressions using .NOT. are evaluated

Messages contain many entities—the subject, body, attachment, MIME content, and so on. An expression using the .NOT. operator does not trigger if any entity in the message does not trigger the expression.

For example, consider the expression *.NOT. cat* evaluated against the following message:

```
Subject = “There once was a cat...” {no match/not triggered}
Body = “who lived in a hat” {match/triggered}
```

The expression *.NOT cat* does not trigger, because there is an entity (the subject) which does not trigger the expression.

In other words, all of a message’s entities must trigger an expression for the message to trigger an expression. Each entity is evaluated against the expression using .NOT., and their results are combined and evaluated using the following logical expression:

```
.NOT operand {entity1} .AND. .NOT operand {entity2} .AND. .NOT
operand {entity3}
```

This evaluation is relevant because when you configure the mail format in some email clients to be HTML, the resulting message has MIME content-type “multipart/alternative,” with a “text/plain” mail body entity and a “text/html” mail body in the same message.

Limiting Operator (.OCCUR.)

.OCCUR. coming soon

This expression matches content and evaluates as true if "coming soon" occurs more than or equal to the preset number of times. The following are some examples if the preset number is 2.

Content	Result
...her birthday is **coming soon**, and I'll buy her a cake...	No match
...her birthday is **coming soon**, and Thanksgiving is also **coming soon**...	Match
...her birthday is **coming soon**, Thanksgiving is **coming soon**, and a hurricane is **coming soon**.....	Match

Table 6-13. Limiting operator [*.OCCUR. coming soon*]

Relational operator

High .NEAR. Sky Diving (.NEAR.)

This expression matches content and evaluates as true if the number of tokens between "High" and "Diving" is less than the preset number. Note that "Sky" counts as one token between "High" and "Diving". If the preset number is 1, the condition is never triggered. The following are some examples if the preset number is 3.

Content	Result	Tokens Between
...**High** Danger Extreme Mountain **Sky Diving**...	No match	5
...**High** Danger Mountain **Sky Diving**...	No match	4
...**High** School **Sky Diving**...	Match	3

Table 6-14. Relational operator [*High .NEAR. Sky Diving*]

Configuring the ASCII/text file exception rules

You can set exception rules to skip ASCII/text file attachment scanning. If you enabled and assigned ASCII/text file extension exceptions, eManager will skip the scanning of this email message attachment content.

To configure the ASCII/text file exception rules:

1. Go to the InterScan MSS install path:

   `\trend\imss\lib`

2. Open the TMeMgr.ini file and modify the following setting:

   To skip all .DXF ASCII type file extension scanning:

   `[em_core]`

   `EnableSkipASCIIFile=yes` (change this value from **no** to **yes**)

Note: "yes" and "no" cannot be upper case.

   SkippedASCIIFileList=dxf

3. Save the TMeMgr.ini file.
4. Restart InterScan MSS.

   The new setting takes effect after you click **Apply Now**.

Note: The default setting disables the scanning of ASCII files. If you want to add file extensions, use the semicolon (;) to separate each extension.

Complex expression example

You may want the eManager filter to detect tokens, except when they appear with other words. This example shows you how to write an expression that can filter successfully under those circumstances.

Scenario

As part of a policy designed to detect suggestive email content, you want to filter for the keyword “breast”. However, you want to exclude legitimate occurrences of this keyword, such as “breast cancer”. Likewise, you may want to filter for the keyword “breasts” but exclude occurrences of “chicken breasts”.

The requirements of this expression are:

1. Detect “breast”, but ignore when part of the expression “breast cancer”.
2. Detect “breasts”, but ignore when part of the expression “chicken breasts”.

Writing the expression

Requirement #1 can be checked by the expression:

```
breast .AND. .NOT. breast cancer
```

Requirement #2 can be checked by the expression:

```
breasts .AND. .NOT. chicken breasts
```

These two expressions could have also been written as:

```
breast .AND. .(..NOT. breast cancer.)
```

and

```
breasts .AND. .(..NOT. chicken breasts.)
```

respectively.

Note: We do not have to use parentheses in the above expressions because the .NOT operator is evaluated before the .AND. operator. For more information, see *Priority of operators* starting on page 6-19.

The final expression

Since we want to detect occurrences of “breast” or “breasts”, we combine the two expressions into one using the .OR. operator.

The final expression is:

```
.(.breast .AND. .NOT. breast cancer.). .OR. .(.breasts .AND.
.NOT. chicken breasts.)
```

Note: The .(. and .). operators are required in the final expression because the .OR. operator has the lowest priority of operation. The evaluation order is not correct if the .(. or .). operators are omitted.

Evaluating expressions

All expressions are evaluated based on the order of operations described below.

Rules

Expression evaluation rules can be summarized as follows:

1. The expression must be valid.
2. Contents in parentheses are evaluated.
3. Contents are evaluated from left to right.
4. Contents are evaluated based on the operators’ precedence.

Valid expressions

The following is a list of the valid expression types:

Type (1)

Operand-only expression (no operator), such as:

```
keyword
```

Type (2)

```
.WILD.  <Type  (1) expression>
```

Note: Due to performance issues, the first token and the last token after the operator ".WILD." cannot consist only of "*", e.g., .WILD. * , .WILD. * Birthday and .WILD. Happy * are all invalid expressions.

Type (3)

```
.NOT. <Type (1) expression>
.NOT. <Type (2) expression>
.NOT. <Type (3) expression>
.NOT. <Type (4) expression>
.NOT. <Type (5) expression>
.NOT. <Type (7) expression>
```

Type (4)

```
.OCCUR. <Type (1) expression>
.OCCUR. <Type (2) expression>
```

Type (5)

```
<Any Type (1 to 7)> .AND. <Any Type (1 to 7)>
<Any Type (1 to 7)> .OR. <Any Type (1 to 7)>
```

Type (6)

```
<Any Type (1 to 2)> .NEAR. <Any Type (1 to 2)>
```

Type (7)

```
.(. <Type  (1 to 7) expression> .).
```

Note: If an expression does not comply with one of the above seven types, it is treated as invalid.

Examples

Expression	Validity	Explanation
.OCCUR. .(. High **.AND.** Low **.).**	Invalid	.OCCUR. cannot appear before Type (7) expression
.NOT. High **.NEAR.** Low	Invalid	.NEAR only can apply to Type (1) and Type (2). .NOT. High is Type 3
.NOT. .(. High **.NEAR.** Low **.).**	Valid	Complies with Type 3
.WILD. better * faster **.NEAR.** coming soon	Valid	Complies with Type 6
.WILD. *	Invalid	The first token, which follows ".WILD." is "*"
.WILD. Hello, every ****	Invalid	The last token, which follows ".WILD." is all *

Table 6-15. Examples of valid and invalid expressions

Using reserved words as operators

To match some reserved keywords (for example, those that use text that resembles an operator in an operand), add an escape character "\".

For example, if you want to match keyword "AAA .AND. BBB", the expression that you can use is "AAA \.AND. BBB". You have to add an escape character on ".AND.", because ".AND." is an operator. If you want to match keyword "\", you have to use expression "\\".

Note: The escape character is not character-based, but token-based. That is, the escape covers the entire token, not just the character. Also, it does not escape the special character asterisk (*) in the expression that follows the .WILD. operator.

Chapter 7

Filtering Content with the Spam Prevention Solution Filter (SPS)

This chapter explains how to use the SPS spam filter in your policies.

Topics include:

- Understanding the spam filter
- Setting the sensitivity of the filter
- Setting confidence levels
- Working with Approved/Blocked Sender lists
- Exempting messages from scanning
- Adding “Spam” to the subject line of messages

Understanding the SPS filter

Spam detection under SPS is based on sophisticated message characteristic processing and analysis technology. Unlike other approaches to identifying spam, such as reference databases of known spam or human editor review, this analysis of message characteristics provides high performance, real-time detection that is highly adaptable, even as spammers change their techniques.

Spammers use a variety of techniques to defeat common detection routines. These include modifying message headers, re-ordering content, and spoofing addresses. A statistical analysis of multiple message characteristics provides the most effective spam detection method.

The spam score

As messages pass through the system, the SPS filter applies thousands of rules against the message envelope, the header, and the content. Each rule is assigned a numerical value, and an equation is formulated based on the weighted significance and the combination of rules that are triggered. The result of this equation is the spam score.

SPS makes a decision on whether the message is spam or valid by measuring the spam score against the desired level of spam sensitivity. Setting the sensitivity higher causes more messages to be considered spam, since increased sensitivity means that a lower spam score will result in a message being considered spam. You can set the overall sensitivity of the SPS filters, as well as fine-tune the sensitivity to different categories of spam.

Categories of spam

If the SPS filter categorizes a message as spam, it will usually fall into one of four categories:

- Sexual content: Adult or pornographic material
- Racist content: Racially insensitive material
- Make money fast: Get-rich-quick material
- Commercial offer: Sale notices, coupons, and special offers

The **Baseline Detection Rate** and the category settings allow the system to derive a sensitivity level based on your company's tolerances.

To set the sensitivity level for the available filters, select **Turn ON Spam filters** and choose the sensitivity of the filter by selecting a level from the **Baseline detection rate**.

Understanding the general and category sensitivity settings

The **Baseline detection rate** is used to determine the overall sensitivity to messages that are potentially spam. Regardless of how individual category sensitivities are set, the **Baseline detection rate** provides a general level of protection against spam. Increasing the setting of one or more of the categories increases the sensitivity to that type of content.

The **Baseline detection rate** and category sensitivity levels are set independently, but parameters from both settings provide the final sensitivity level that determines whether the message is categorized as spam. Category sensitivity levels multiply the **Baseline detection rate** and increase the likelihood that a message that triggers a category setting will be considered spam.

Selecting an SPS engine option

SPS now incorporates new technology aimed at helping you configure spam filtering to better match your organization's messaging environment. You can set SPS to detect spam based on the following:

- Select **Default** to use the default SPS engine
- Select **Engine option trained by multi-lingual spam samples** to configure SPS to take regional spam variations into account
- Select **Lower false positives** to reduce false positives (reduces false positives, but reduces the overall catch rate)
- Select **Higher catch rate** to increase catch rate (catches more spam, but increases the likelihood of false positives)

Setting category sensitivities

If the spam score for a given message exceeds the sensitivity level of your policy, the message is considered spam. There are three exceptions to this:

- If the sender appears on the **Approved Senders** list, the message is never considered spam.
- If the sender appears on the **Blocked Senders** list, the message is always considered spam.
- If text in the message triggers a **Text Exemption Rules**, the message is never considered to be spam.

The definition of spam varies, so messages that are considered spam at your organization might have value at another. The category settings allow you to fine-tune the sensitivity. For example, if your organization has a zero-tolerance policy for sexual content, but allows commercial offers (such as “trips to Hawaii on sale”), set the **Sexual content** to the most sensitive value (high), and set the **Commercial offer** sensitivity to a lower level (lowest or low).

Setting the action for categories

Each of the categories can have a different action based on the particular needs of users. For instance, you may want to delete messages classified as make money fast, but you may want to quarantine sexually explicit or racially insensitive email for later investigation.

To set the actions for the categories:

1. From the **Policy Manager**, select **Edit** under the **Filter Action** column for a SPS filter.
2. Choose an action for each confidence level:

   Select **Default** to have the default action applied to messages that match a particular category. For instance, if the Baseline action is **Delete**, set the action for **Make money fast** to **Default** to delete those messages that the SPS filter determines are in the **Make money fast** category.
3. Click **Save.**

Setting levels of confidence

The actions for SPS filtering can be set based on how confident the system is of its determination that a particular message is spam. For instance, you might choose to have the system delete messages in cases where there is a high level of confidence that the message is spam containing sexual content, but quarantine messages where it is only moderately confident.

To set the confidence levels:

1. From the **Policy Manager**, select **Edit** under the **Filter Action** column for a SPS filter
2. Select the **Advanced** link or the arrow next to the category you want to adjust
3. Choose an action for each confidence level

   Select **Category Default** to have the default action for that category applied to messages that match a particular confidence level. For instance, if the **Make money fast** category's action is **Delete**, set the action for **Most Confident** to **Category Default** to delete those messages that the SPS filter is most confident fall into the Make money fast category
4. Click **Save.**

Working with Approved/Blocked Senders lists

Two exceptions to the message evaluation process are:

- If the sender appears on the **Approved Senders** list, the message is not scored; it is not treated as spam.
- If the sender appears on the **Blocked Senders** list, the message is not scored; it is treated as spam.

Note: Approved and Blocked Senders lists apply only to the SPS filter

Understanding Inheritance

Approved/Blocked Senders lists follow the standard hierarchical Policy Manager inheritance model. As long as an address in a child policy is a subset of the address in a parent policy, and the parent policy has set the address as **Modifiable**, the child can remove the item, "specialize" the item, and add it to the opposite list. So, for instance:

If the parent policy has blocked `*@domain.com` as **Modifiable**, the child policy can approve `john@domain.com`.

If the parent policy has blocked `*@domain.com` as **Unmodifiable**, the child policy cannot approve `john@domain.com`.

Filters at the peer level follow this same model, with one exception: if you enter the same address in both the Approved Senders and Blocked Senders lists, address in the Approved Senders list will have priority.

When viewing addresses in the Approved or Blocked senders lists, addresses that were added at the policy level are in black, and addresses inherited from a parent policy appear shaded.

Modifying Approved or Blocked senders lists

To modify the addresses in the **Approved** or **Blocked senders** lists:

1. From the policy tree, select a SPS filter and under **Type**, click **Edit**.
2. From the **Spam Filter** page, click **Edit** next to the list to modify.

Note: You cannot modify addresses in sub-policies if they are set as **Unmodifiable** in the parent policy.

---

3. To add an address, enter the address in the **Add email addresses** text area and click the ⊕ button.

Note: To add addresses from an existing list, you may paste multiple addresses separated by commas, semicolons, or spaces.

---

4. To delete an address, select the address from the Address list text area, and click the − button.
5. To save your changes, click **Save**.

Using the * wildcard in Approved/Blocked Sender lists

Approved/Blocked Sender list entries may include wildcard characters. Wildcards allow you to configure the Approved/Blocked Sender lists to match multiple addresses with a single entry.

- Using * in an expression

  The behavior of wildcard * differs whether it appears before or after the @ in an email address. Text that comes before the @ is treated as the name; text that comes after @ is treated as the domain. If no @ exists, then the entire string is considered invalid. For example, strings such as “abc” or “trendmicro.com” are invalid. Approved/Blocked Sender list entries are validated as they are entered, and invalid entries are rejected.

- Name Pattern

  To match the name, you can only use a single wildcard * or the exact name. Partial matches are not allowed. The wildcard matches everything except no entry in the field.

  For example:

  - *@trendmicro.com matches stanley_edwards@trendmicro.com
  - Joe*@trendmicro.com or *edwards@trendmicro.com is not allowed

- Domain Pattern

  For the domain, the wildcard * can only occur at the beginning of the pattern, and it can match one or more subdomains. You can use multiple wildcards to match subdomains.

  For example:

  - *@*.solar.com matches *@earth.solar.com
  - *@*.solar.com matches *@europe.earth.solar.com
  - *@*.solar.com does not match *@solar.com

Partial matching of subdomains is not allowed. You must enter wildcards from the most significant portion of the address to the least significant. For example, *@trend.*.com is an invalid format, but *@*.trend.com is valid.

Adding “Spam” to the subject line

Using the SPS filter, an additional filter action is available, called **Tag and Deliver**. By selecting **Tag and Deliver** from the filter actions drop-down, messages SPS identifies as spam will have “Spam: ” prepended to the subject line. For example, if the original subject line is “Work at Home!”, when this feature is enabled the subject line is changed to, “Spam: Work at Home!” When SPS tags a message, it can be deleted by recipients can delete the message without taking time to open and read it.

Note: The **Tag and Deliver** action is only available for the SPS filter

Using text exemption

There may be times when you want to allow email delivery based on certain keywords. For instance, if there are messages from a particular on-line discussion group that is advertising-sponsored, and those messages are consistently identified as spam, you might want to exempt all messages that contained the text “DanSoft Discussion Group” from spam filtering. SPS provides text-exemption for the SPS filter that exempts messages from filtering if they contain a specific keyword or combination of keywords.

Note: Text exemption applies *only* to SPS filters and applies across *all* SPS filters rather than by individual policy.

To create a text-exemption rules:

1. Navigate to one of your SPS filters (the text exemption rules apply across all policies that contain an SPS filter).
2. Open the text exemption page by clicking **Text exemption rules**.
3. Click **New Rule** and enter a name for the new rule.
4. Select the areas of messages to scan.
5. Enter the string(s) to match.
6. Click **Save Rules** to save your changes.

Fine-tuning the SPS Filter

To obtain the maximum effectiveness from SPS, “tune” the filters according to your organization’s definition of span and your users’ need for unique exceptions. The goal is to account for messages that might be incorrectly classified as spam, based on their characteristics, by adding exceptions that allow you to increase the sensitivity of the filter without fear of false positives. Make exceptions by adding addresses to the Blocked and Approved Senders lists, as well as creating Text exemptions.

It is best to adjust the SPS filter in small steps, rather than making numerous large changes at once. Follow these general guidelines:

- If there are many junk email messages getting through the SPS filter, increase the **Baseline detection rate** sensitivity.

  The lower the **Baseline detection rate** sensitivity setting is, the higher a category filter setting will have to be to have an noticeable effect.
- When you increase the **Baseline detection rate** sensitivity, reset the category filter sensitivities back to **Lowest.** Monitor your message flow and then increase the category sensitivities as necessary.
- Setting the filters at too high a level can result in valid messages being falsely identified as spam. While setting the **Baseline detection rate** sensitivity high can result in some valid email messages being falsely identified as spam, it should result in fewer false positives than setting an individual category filter too high.

Tuning the Spam Filter

1. Start with the default sensitivity values.

   Trend Micro recommends starting with the default value of **1 - Most conservative** for the Baseline detection rate and **Lowest** for the category filters. The only exception is when an organization is particularly sensitive to a particular category of spam.

Note: Some message recipients may be particularly sensitive to certain types of spam. If this is a concern, the initial values for the appropriate categories should be raised to be more aggressive for these types of emails.

---

2. Set the filter action for messages where SPS is less confident to **Tag and Deliver**. See *Setting levels of confidence* starting on page 7-6 and *Setting the action for categories* starting on page 7-5 for details.
3. Monitor email.

   While tuning the SPS filters, carefully monitor the logs and quarantine areas to see how various types of messages are being processed.
4. Request feedback from message recipients.

   During the tuning process, solicit the cooperation of message recipients and ask that they send examples of messages that were not correctly identified, including valid messages tagged as spam and spam that was not tagged. This information is useful when adjusting filters. It can also tell you whether you need to create entries in the Approved Senders and Blocked Senders lists or Text exemptions.

Note: When a user finds a false positive or negative, they should forward the email to the administrator with all headers intact. The headers can help with understanding why a message was or was not considered spam and to determine the course of action to follow. Note that some email clients will remove some or all of the message headers when forwarding.

---

5. Analyze processed messages.

   Look carefully at the content of messages that are incorrectly classified to determine which category sensitivities to adjust.
6. Adjust sensitivity levels.

If spam is not detected at default levels, first change the **Baseline detection rate** to **2 - Conservative**. If spam is still being missed, increment the sensitivity settings in the category where the misses occurred. Continue incrementing the level until spam is consistently identified.

If false positives occur, consider decreasing the sensitivity setting in the category where the false identification occurred, or adding the sender to the Approved Senders list. If the sender is a mailing list, someone who often sends mail that resembles spam, or a trusted sender, it is better to use the Approved Senders list.

7. Repeat.

   After you have adjusted the settings, repeat steps 2 through 5 until you have reached an appropriate level of spam sensitivity.

8. When you have adjusted SPS to an appropriate level of sensitivity and your message recipients are not seeing valid mail tagged as spam, set the filter actions for less confident spam to **Quarantine** or **Delete**.

Order of evaluation for SPS

When a message is evaluated by SPS, the order is:

1. The Approved Senders and Blocked Senders lists are checked first. Non-modifiable entries are checked before modifiable ones, and then the appropriate list is selected based on the best match.

   If the message sender's address appears on the Approved Senders list, the message is passed to the next InterScan MSS filter for evaluation and SPS does no further processing of the message. If the sender's address appears on the Blocked Senders list, SPS performs the action assigned for blocked senders.

2. Text Exemption matching is evaluated.

   If the sender's address is not on the Approved Senders or Blocked Senders list, the message content is evaluated for a match to a Text Exemption rule. If the message matches a Text Exemption rule it is passed to the next InterScan MSS filter for evaluation and SPS does no further processing of the message.

3. The message is evaluated based on the SPS settings and the message is assigned a spam score. SPS performs the appropriate action based on the score.

Note: If you are using Trend Micro ScanMail for Exchange (SMEX) with spam quarantining, or Trend Micro AntiSpam, the Microsoft Outlook plug-in for spam management, spam message handing will depend on policy settings across all products. For instance, IMSS may be configured to tag and deliver spam messages, but Trend Micro AntiSpam may be configured to move them to the spam folder. In this case, a message "delivered" by IMSS to the end user will still be placed in the spam folder.

Chapter 8

Centralized Reporting and Web-based End User Quarantine

This chapter explains how to use the centralized spam reporting and end-user quarantine management console with InterScan™ Messaging Security Suite to provide centralized reporting and Web-based End User Quarantine (EUQ) spam quarantine management.

Topics include:

- Understanding the Web quarantine tool
- Enabling end-user access to the spam quarantine
- Working with the consolidated spam reports
- Configuring the database

Understanding Centralized Reporting and Web-based End User Quarantine

The Centralized Reporting and Web-based End User Quarantine component of InterScan™ Messaging Security Suite provides an administrative console that allows administrators to configure spam reports across all IMSS servers and to configure end user access to messages quarantined as spam. A separate component, the end user console, allows end users to log in to a Web server and manage messages that InterScan MSS has quarantined as spam. These services require a license to Trend Micro's Spam Prevention Solution (SPS).

Working with the Web-based EUQ tool

In conjunction with SPS, the Web-based end-user quarantine tool allows end users to manage messages in their spam quarantine area. You can allow end users to sort borderline suspicious messages, relieving messaging administrators of this task. This is important, because spam definitions are subjective.

While one user might consider messages from an online retailer to be spam, another user, who has a relationship with the retailer, might consider such messages legitimate. The Web quarantine tool empowers users to identify this "gray-area" of messages that might be considered spam by some users and legitimate messages by others. Allowing users to classify these messages reduces the number of requests that administrators will need to deal with concerning possible spam messages.

You must have configured your network to allow the Web quarantine tool to connect to your LDAP server to use the Web quarantine feature. This allows the Web quarantine tool to use LDAP accounts to authorize access to quarantined items.

Note: If your LDAP server requires connections to use Kerberos authentication, your servers must be time-synchronized.

You must also have installed a PostgreSQL database to index spam messages for end user retrieval. A PostgreSQL installer is included in the installation package. You may also use a pre-existing instance of PostgreSQL as your database software.

Note: To enable spam message indexing, you must configure the database settings in the IMSS Web console. These settings can be found under **Configuration** > **Database Settings**.

Installing the EUQ Admin component

To use the Web quarantine tool, you must have installed a database and the Central Reporting / Web-base quarantine component. This component provides two Web servers, one allowing administrators to configure the console and another allowing users to access their spam messages. Follow the installation instructions in this Getting Started Guide to install the end-user quarantine tool.

- The installation program configures the Web quarantine to listen on port `8447` for the administration console and on port `8446` for end user traffic.
- When IMSS receives a message with a single recipient, it quarantines the message and flags it as spam for that user/recipient.

Understanding how Web-based end user quarantine fits into your network environment

The server where you install the Web quarantine must be able to connect to both your LDAP server for user validation, and the IMSS database. In addition, your users must be able to access this server using their Web browser.

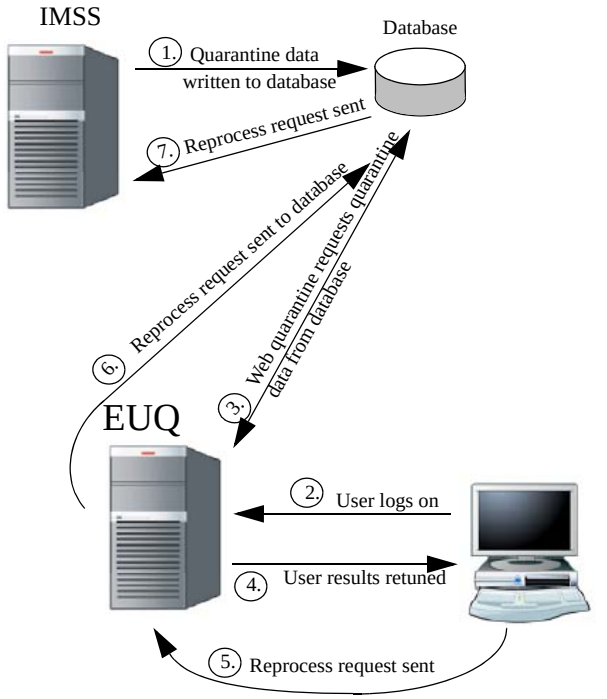


Figure 8-A: Web quarantine topology where components are on different servers

Note: The database can be installed on the same server as IMSS, the same server as the centralized spam reporting and EUQ components, or on another server. As long as you have correctly configured your network and the DNS so that the components can connect to the database, it can be located wherever you choose.

Enabling Web-based end user quarantine access

The installation program does not automatically enable Web quarantine after installation. If your users will be accessing the Web quarantine tool, you will need to enable and configure it.

Note: You must have configured the IMSS server(s) to write spam data to the database to enable Web-based EUQ.

To enable Web quarantine access:

1. Open the centralized spam console on the server by typing the server URL and port number (8447) in your Web browser.

   For example, `https://127.0.0.0:8447`
2. Type the password. The default password is `imss`
3. Configure LDAP connection settings by clicking **Web Spam Quarantine** > **LDAP Settings** in the left navigation panel.
4. Click **Save** to save your settings and test the LDAP connection.

   Note: If you change to a different LDAP server, restart the Spam Console service to allow the new setting to take effect.

   ---
5. Open the End-User Access screen in Web console by clicking **Web Spam Quarantine** > **End-User Access** in the left navigation panel.
6. Set the **Approved Senders Setting** for each Web quarantine user. This is the maximum number of approved senders that each end user can set.
7. Select **Disable end-user access** to disable this feature.
8. Select **Enable end-user access for all LDAP users and groups** to enable access for all LDAP entities.
9. Select **Enable end-user access for selected LDAP groups** to enable access for a subset of LDAP entities.
   a. Select users and groups from the **Select LDAP groups to enable access** field.

b. Type a group or user name in the **LDAP Search** field and click **Search** to find users or groups.

c. Click **Add** to move user and groups to **Selected Groups**.

10. Click **Save**.

Understanding message handling

- When IMSS receives a message with multiple recipients, and only one policy applies to all the recipients, it quarantines the message and flags it as spam for all users/recipients. However, in this case, IMSS counts this as a single processed message.
- When IMSS receives a message with multiple recipients, and different policies apply to different recipients, it quarantines the message and flags it as spam for all users/recipients. However, in this case, IMSS "breaks" the message into multiple copies to enforce the appropriate policy based on the recipients/users.

For instance, assume InterScan MSS receives a message sent both to *dan@example.com*, with a policy that includes a spam rule, a virus rule, and a content rule, and to *jennifer@example.com*, with a policy that contains only a spam filter and a virus filter. To process the two different policies, InterScan MSS copies the message and applies the *dan@example.com* policy to the original, and the *jennifer@example.com* policy to the copy.

Understanding the message quarantine process

When InterScan Messaging Security Suite processes a message using the SPS filter, if the message is determined to be spam and the action for spam is quarantine, the message is placed in the appropriate quarantine directory on the IMSS server where it was processed. Periodically (every three minutes, by default) the Web quarantine agent on the IMSS server checks for newly quarantined spam messages. It then indexes the quarantined messages in the Web quarantine database. Once the messages have been added to the database, end users can access them through the Web-based quarantine tool.

Understanding Message Expiration

When messages are quarantined by an SPS filter, the amount of time that they are stored in the quarantine area is based on the settings for that quarantine area. For instance, if the quarantine expiration is set to 10 days, spam messages will be stored in the spam quarantine, and accessible to the end user, for 10 days. Once the message reaches the expiration limit, it is deleted from the database as well as from the hard drive where it is stored.

Note: If you set the quarantine expiration to “Unlimited” the message files will never be deleted from the hard drive. However, to prevent database problems, messages that are in quarantine areas are deleted from the database after 15 days, no matter how the quarantine expiration is configured.

Web quarantine login information for end users

Each Web quarantine user will log on to the Web quarantine interface using their LDAP `userPrincipalName` as their username. It is important to clearly explain this to your users so that they do not attempt to log on to the Web quarantine interface using just the user portion of their account name. Specifying their full distinguished name provides the necessary domain information to enable the Web quarantine server to look up their user information through LDAP.

Note: The Web quarantine tool uses the users `userPrincipalName` to look up the email address stored under the “mail attribute” in LDAP. Quarantined messages sent to the “mail attribute” address(es) are displayed when the user logs on with the associated `userPrincipalName`.

For example, a user that logs on to their Windows desktop account with a username of `danielh` actually specifies the domain at login. When accessing the Web quarantine interface, this user would use `danielh@us.example.com` as their username, allowing the Web quarantine to correctly look up their LDAP account information by referencing the `us.example.com` domain. If the `danielh@us.example.com` user principle name is in an LDAP record with a mail attribute of `danielh@us.example.com`, the Web quarantine tool will display all quarantined spam that has a recipient address of `danielh@us.example.com`.

If you change the LDAP server settings to point the Web quarantine tool to a different LDAP server after initial configuration, it will affect the user access and log in information unless the servers contain identical users and groups. Trend Micro does not recommend changing LDAP server settings after installation.

Allowing Multiple Email Addresses Per User

In a MicroSoft Exchange environment, where Exchange and Active Directory are on the same server, you can allow multiple addresses for a single Web quarantine user by modifying the Active Directory record for that user to include all the appropriate addresses in the `proxyAddresses` attribute. Exchange automatically extends the Active Directory schema to allow multiple addresses. This allows the Web quarantine tool to access all messages for each address in the `proxyAddresses` attribute.

Once you have configured Active Directory, edit the IMSS database. In the tb_global_setting table, locate the mail_attribute field. The default value of this field is “mail.” Change the value of the mail_attribute field to “proxyAddresses” (without the quotes) to enable support of multiple e-mail addresses.

Note: After you have changed the database, you must restart the IMSS EUQ console service to enable the change.

Managing approved sender lists

You can see the current total number of approved senders on the Web quarantine management screen. This number is the total number of approved sender list entries for each user of IMSS. Users also see this total when they log on to access their personal quarantine area.

Note: If you set the total number of approved sender list entries to a number that is lower than the current setting, end-users who have more than that number of entries will have their approved sender list truncated the next time they access Web quarantine, with the oldest items being deleted first. Trend Micro suggests informing end-users of this action, to preempt user questions about “missing” entries.

Understanding user and administrator interaction

Each message processed by InterScan Messaging Security Suite and quarantined by an SPS filter is flagged in the IMSS database as being available for end users to view through the Web quarantine console. Understanding the way that IMSS handles these messages will help you when working with Web quarantine or when it is necessary to troubleshoot the Web quarantine tool.

For each received message that triggers the spam filter, there are several possible outcomes that are determined by the recipient address(es) and the InterScan MSS policies that apply to them:

- When IMSS receives a message with a single recipient, IMSS quarantines the message and flags it as spam for that user/recipient.
- When IMSS receives a message with multiple recipients, and only one policy applies to all the recipients, it quarantines the message and flags it as spam for all users/recipients. However, in this case, IMSS counts this as a single processed message.
- When IMSS receives a message with multiple recipients, and different policies apply to different recipients, it quarantines the message and flags it as spam for all users/recipients. However, in this case, IMSS "breaks" the message into multiple copies to enforce the appropriate policy based on the recipients/users.

  For example, assume InterScan MSS receives a message sent both to *dan@example.com*, with a policy that includes a spam rule, a virus rule, and a content rule, and to *jennifer@example.com*, with a policy that contains only a spam filter and a virus filter. To process the two different policies, InterScan MSS copies the message and applies the *dan@example.com* policy to the original, and the *jennifer@example.com* policy to the copy.

These different outcomes affect the way that InterScan MSS handles messages that are quarantined as spam. If InterScan MSS splits the message into multiple copies, when the administrator deletes a message from one end user's spam quarantine, it has no effect on the copies. However, IMSS does not split the message, and the message belongs to two recipients *dan@example.com* and *jennifer@example.com* then:

- If *dan@example.com* opens the Web quarantine console and deletes the message, *jennifer@example.com* will still see this message if she opens the Web

quarantine console. Administrators using the Web console's quarantine search tool will still be able to see this message.

- If both *dan@example.com* and the *jennifer@example.com* have used the Web quarantine console to delete the message, administrators using the Web console's quarantine search tool will not see it.
- If an administrator deletes the message from the Web console's quarantine search tool, the users *dan@example.com* and *jennifer@example.com* will see the message information, but will be unable to see the message details.

Working with the web quarantine tool

InterScan MSS allows users to take control of their own messages that have been identified as possible spam. This enables administrators to move the burden of identifying possible spam messages and releasing them to the end user. The instructions below explain how to provide Web quarantine access to end users, as well as describing the use of the Web quarantine tool for end users.

Opening the IMSS web quarantine tool interface

Your end users can view the InterScan Messaging Security Suite Web quarantine console with a Web browser.

To view the console in a browser, go to:

```
https://<IMSS_server (or IP)>:8446
```

For example, if your server's IP address is 127.0.0.0, you would type:

```
https://127.0.0.0:8446
```

An alternative to using the IP address is to use the target server's fully qualified domain name (FQDN). Because the end-user management console uses SSL for security, you must type "`https://`" before the domain name and append the port number after it.

If the FQDN of you server is long, or might be hard for end-users to remember, Trend Micro suggests creating a redirect page at a more "friendly" URL address and providing that to users, or providing a link to the Web quarantine tool from your organization's intranet or portal.

Note: Trend Micro recommends enabling Web quarantine for a single account and then testing the Web quarantine console before enabling it for all users and sending out the Web quarantine instructions.

Instructing end users

The InterScan MSS installation package provides a Web Quarantine Guide for end users. There are two versions of this guide. One is a plain-text document that provides basic instructions on interacting with the InterScan MSS Web quarantine interface in ASCII text, similar to a readme. You can distribute this document to your users as an email message. The second is a PDF that contains the content included on the following two pages, which you can distribute as necessary.

Note: Before distributing these messages, edit the URL to reflect the actual URL that your users need to use to access the Web quarantine tool.

In addition to the end user guides, the Web quarantine tool itself provides help files that user can access directly from the Web quarantine interface. These help files are automatically installed during the Web quarantine server installation.

Using the web quarantine tool

InterScan MSS allows you to take control of your own messages that have been identified as possible spam. This means that you can identify possible spam messages and decide to release or delete them at your convenience. The instructions below explain how to use the Web quarantine tool.

Opening the web quarantine management console

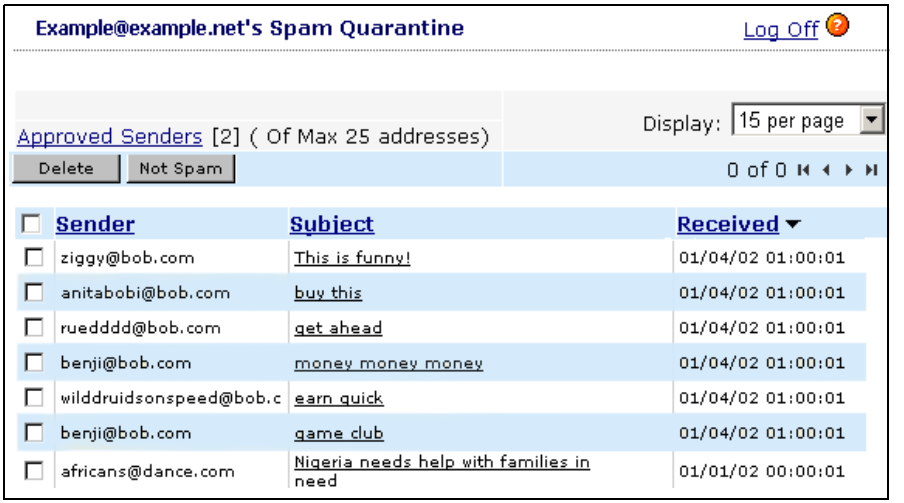
Your administrator should provide you with a URL that will allow you to access the Web quarantine console. Open your browser and type that address into the **Address** field to open the console. You may also want to add the address to your bookmarks to make accessing the tool easier in the future.

To open the web quarantine management console:

1. Open your Web browser.
2. Navigate to the address your administrator provided.
3. Type your username and password.
4. Click **Login**.

Viewing quarantined messages

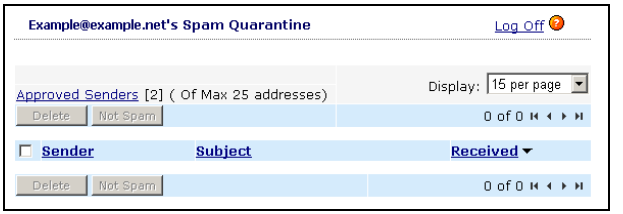
When the console opens, you will see the main page, which provides a list of messages that were sent to you that are in the quarantine. From here, you can delete them or tag them as Not Spam.



Managing quarantined items

The main page lets you see messages that have been placed in the quarantine. You can use the viewer to take different actions depending on whether a particular message is spam or not.

Each message that is identified as spam is shown in the list at the bottom of the screen. This list tells you who sent the mail, the subject, and the date and time the message was received



Viewing a message

If you can't tell from the message sender and subject alone if a message is spam, you can open the message and look at the contents.

To view the entire message:

1. Click the message subject.
2. This will open the message viewer.

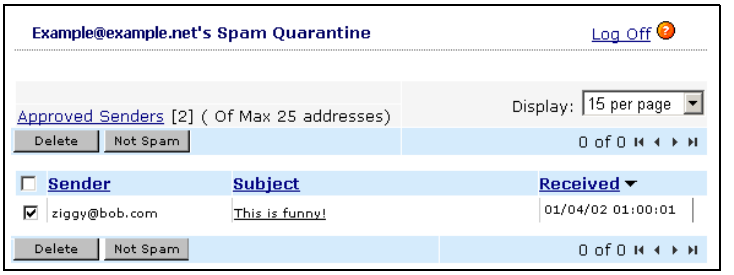
3. From here, you can choose to delete the message or add the sender to the Not Spam list.
4. To close the message viewer, click **Back to List**.

Deleting spam

If you have identified one or more quarantined messages as spam, you can easily delete them.

To delete a message:

1. Select the message by clicking the checkbox in the same row as that message



2. Click the **Delete** button at the top of the page.

Note: You can delete multiple messages by selecting them in the same way. To select all the messages that are currently being displayed, click the checkbox at the top of the column.

Releasing messages from the quarantine

If you have identified one or more quarantined messages as not being spam, you can easily release them from the spam quarantine

To release a message:

1. Select the message by clicking the checkbox in the same row as that message
2. Click the **Not Spam** button at the top of the page to process the message for delivery.

Note: You can select multiple messages by selecting them in the same way. To select all the messages that are currently being displayed, click the checkbox at the top of the column.

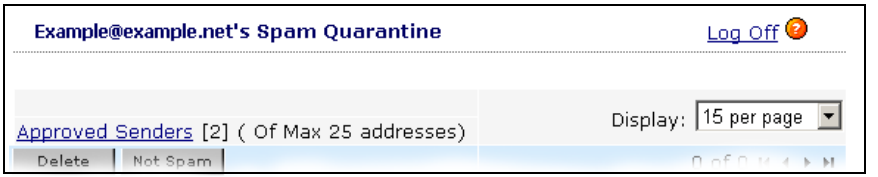
Managing approved senders

InterScan MSS allows each user to add sender addresses and domains to an individual Approved Senders List that prevents messages from these senders from being identified as spam. For example, if you add *joe@example.com* to your

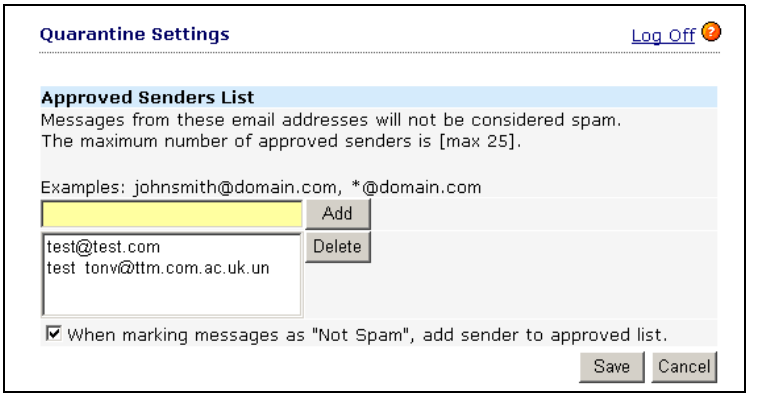
approved senders list, future messages from *joe@example.com* will not be quarantined as spam.

To add senders to your personal approved senders List:

1. Click the **Approved senders** link near the top of the screen.



2. The **Quarantine Settings** screen will open.



3. Enter the email address in the address field and click **Add**.
4. Repeat until you have added all the addresses that you want to the approved senders list, or until you reach the maximum number of approved senders allowed.
5. You can choose to have sender addresses automatically added to your approved senders list when you mark them as Not Spam, by selecting the **When marking messages as "Not Spam," add sender to approved list** check box.
6. Click **Save**.

To remove senders from your personal approved senders List:

1. Select the email address in the **Address** field and click **Delete**.

   Note: To select multiple addresses, hold down the **Ctrl** key.

2. Click **Save**.

Logging out

When you have finished viewing your messages, be sure to log out before closing your browser or navigating away from the Web quarantine console.

To log out:

1. Click the **Log Off** link in the upper right corner of any screen.

2. When the confirmation screen opens, you are logged out of the Web quarantine console and can close your browser.

Using the centralized spam reporting tool

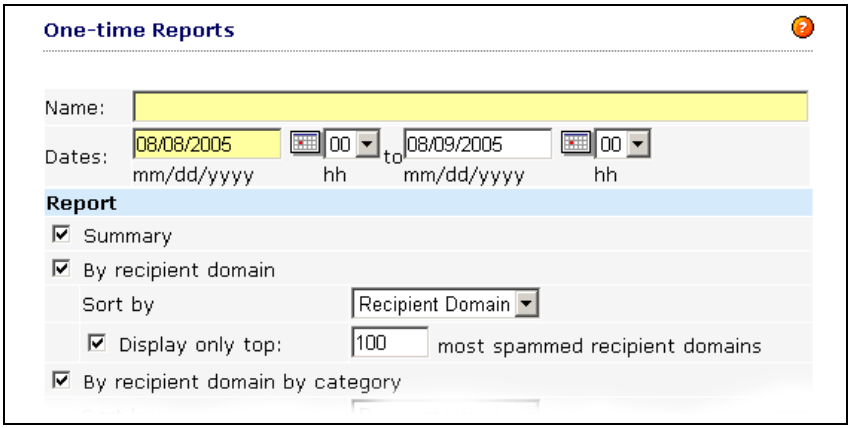
The reporting capabilities of InterScan Messaging Security Suite allow you to monitor messaging traffic and the effect of spam policies. You can generate these reports on a preset schedule, or as needed. You can configure them to provide an overall summary, or detailed information. IMSS generates reports as HTML or CSV files you can view from any browser, save locally for later viewing, or open in word processing software for editing and publishing.

Configuring One-time Reports

IMSS reports are flexible and configurable to meet your organization's reporting needs. InterScan Messaging Security Suite generates scheduled reports at preconfigured intervals, or one-time reports on demand.

To configure a one-time report:

1. Open the One-time Report screen by clicking **Spam Reports > One-time** in the left navigation panel.
2. Click **Add** to configure a new one-time report
3. Configure the report settings:



- **Name** the report
  Trend Micro suggests using a name that represents the type of rule and its settings, for instance: *foo_global_spam_report*.

- Select **By recipient domain** to generate a report broken down by domains, or deselect to generate an aggregated report
- Configure the report contents

Note: Each section provides data only for the period covered by the report. For instance, the **Spam Summary** in a daily report provides a summary of policy events for that day only.

4. When you return to the One-time Reports screen, the report status will be **Pending**. Depending on system resources and other factors, it may be up to five minutes before report generation begins, at which time the status will change to **In Progress**.
5. Click **Save**.

Working with Scheduled Reports

IMSS provides administrators the ability to run reports on a pre-scheduled or as-needed basis. Reports allow administrators to track system performance, messaging throughput, and the effect of rules on messaging. These reports can be scheduled to run during low-traffic times to balance the database queries required for report generation with those needed for message processing.

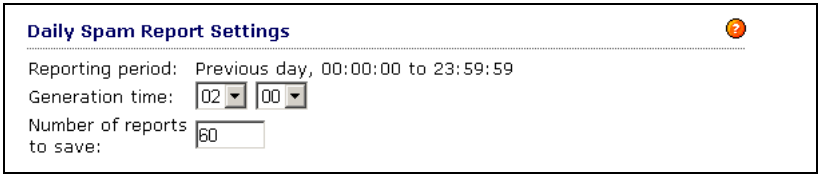
Some InterScan MSS reports are run on a schedule. You can configure them for generation on a daily, weekly, or monthly basis. Trend Micro strongly recommends configuring report generation for non-peak messaging traffic times as generating exhaustive reports that require numerous calls to the IMSS database (generating a report on all policy events for all users this month, for example) can adversely affect message throughput.

Scheduling Reports

There are three types of scheduled reports: daily, weekly, and monthly. You can schedule one report of each type. Once you have configured a scheduled a report, it will be generated at the scheduled time until the schedule is changed.

To schedule a report:

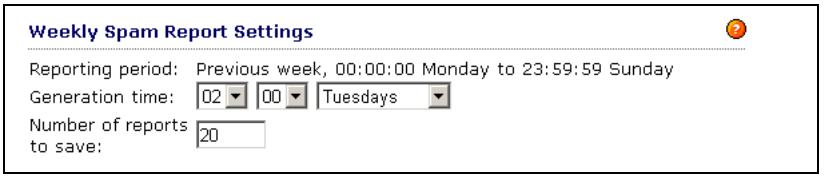
1. Open the Scheduled Reports screen by clicking **Spam Reports > Scheduled** in the left navigation panel.
2. Click **Settings** to the right of **Daily reports** to configure daily reporting.



   a. Configure a **Generation time**—this will be the time that report generation will begin.

   b. Select the data types to include in the report.

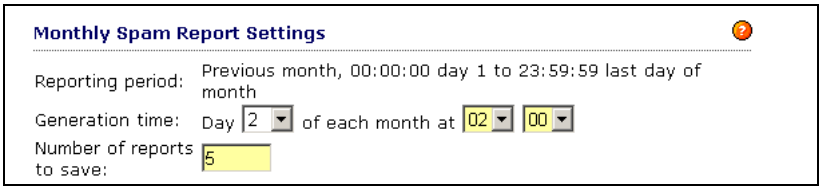
3. Click **Settings** to the right of **Weekly reports** to configure weekly reporting.



   a. Select a time and day of the week that the reports will be generated from the **Generation time** dropdowns.

   b. Select the data types to include in the report.

4. Click **Settings** to the right of **Monthly reports** to configure a monthly report.



   a. Select a day and time under **Generation time** to schedule monthly reports.

Note: If you select 29, 30, or 31, IMSS will generate the report on the last day of the month for months with fewer days. For example, if you select 31, IMSS will generate the report on the 28th (or 29th) in February, and on the 30th in April, June, September, and November.

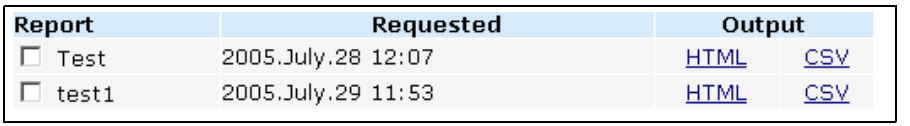
---

   b. Select the data types to include in the report.

Viewing One-time or Scheduled Reports

All generated reports are saved onto the hosting server's disk drive for later viewing. You can review these reports any time after InterScan MSS has generated them from the Reports screen. Generated reports are available from the appropriate screen in either HTML or CSV formats.

Since one-time reports may require some time to generate, they may not be available immediately. Reports that administrators have requested will appear on the Reports results screens with the **Output** status as **In Progress**.



Report	Requested	Output	
☐ Test	2005.July.28 12:07	HTML	CSV
☐ test1	2005.July.29 11:53	HTML	CSV

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.

To view a report:

1. Open the Reports screen by selecting **Reports > One-time** or **Reports > Scheduled Reports** in the left navigation panel.
2. IMSS will display a list of reports.

Note: Reports that are in process will have their **Output** status set to **In Progress**.

---

3. Click the **HTML** hyperlink to the right of the report name.

   A new window will open to display the report.

To download a CSV version of a report:

1. Open the Reports screen by selecting **Reports > One-time** or **Reports > Scheduled Reports** in the left navigation panel.
2. Right-click the **CSV** hyperlink to the right of the report name.
3. Choose **Save target as** from the context menu.
4. The **Save file** dialog will open.
5. Choose a download directory and type a file name.
6. Click **Save**.

Deleting Reports

InterScan Messaging Security Suite saves all reports onto the hosting server's disk drive for later viewing. Regularly purge these reports after you have viewed, saved, or printed them.

To delete a report:

1. Open the Reports screen by selecting **Reports > One-time** or **Reports > Scheduled** in the left navigation panel.
2. Select the check box next to the report(s) that you want to delete.
3. Click **Delete** to delete a single report, or **Delete All** to delete all reports.

Chapter 9

Troubleshooting and Contact Information

This chapter contains information about how to troubleshoot your InterScan MSS installation. In addition, the following Trend Micro technical support services are introduced:

- Installation-related issues
- Notification-related issues
- Obtaining an Activation Code to upgrade InterScan MSS™ from the evaluation period
- Trend Micro's Security Information Center
- Technical support contact information
- Knowledge Base

Troubleshooting

The following information can help you troubleshoot InterScan MSS installation and notification problems.

Installation-related error messages

The following is a list of the error codes that can occur during the CCGI installation:

Error Code	Platform	Message
0	Solaris and Linux	Successful execution.
103	Solaris and Linux	Failed to install CCGI.
104	Solaris and Linux	Administrator rights are needed to perform this installation.
106	Solaris and Linux	Administrator's rights are needed to perform this uninstallation.
107	Solaris and Linux	Insufficient disk space.
121	Solaris	Some patches must be installed before this installation.
148	Solaris and Linux	Uninstallation has been cancelled.
149	Solaris and Linux	Insufficient arguments
151	Solaris and Linux	Could not read the specified configuration file.
152	Solaris and Linux	The configuration file is not well-formed.
153	Solaris and Linux	Bound to ports less than 1024, CCGI service must run as root.
154	Solaris and Linux	Invalid options.
201	Solaris and Linux	Could not create the installation target directory.
202	Solaris and Linux	Could not extract CCGI files.

Error Code	Platform	Message
203	Solaris and Linux	Could not add group.
204	Solaris and Linux	Could not add user.
205	Solaris and Linux	Could not add user to this group.
206	Solaris and Linux	Could not install under directory / or /usr.
221	Solaris and Linux	Failed to finish configuration.
249	Solaris and Linux	Interruption.

TABLE 9-1. Error Codes for the Installation/Uninstallation Program

Notification-related

Using InterScan MSS as notification server may cause message looping

If a content management filter sends an email notification with the original message attached, and InterScan MSS is used as the notification server, an infinite loop occurs. This is because the original message is attached to the notification email message and is tested by all filters when processed by InterScan MSS, which triggers the same filter again. Another notification is sent, attaching the original, the filter is triggered, and so on.

We recommend that you do not use the InterScan MSS server as your notification server.

Registering your product

When the InterScan Messaging Security Suite Web console starts for the first time, it opens directly to the product activation page.

WARNING! Until you activate InterScan MSS, it does not perform any scanning.

In order to activate IMSS or the Spam Prevention Solution, you need to enter a valid Activation Code for each product. There are several ways to obtain an Activation Code:

- As part of the product download
- Through a reseller
- Directly from the Trend Micro Web site

To enter your Activation Code:

1. Go to the product license page by clicking **Configuration** > **Product Licenses**.
2. Click the product you want to activate.
3. Enter your Activation Code.
4. Click OK.
5. When you return to the Product Licenses page, the status of the product you activated will be changed to **Active**.

Note: If you do not have an Activation Code, obtain one by registering your product. This can be done online through the Trend Micro Web site. You will need to provide your registration key (if applicable) and email address, along with additional registration information. Once you have completed the product registration process, you will receive an Activation Code by email, typically within 20 minutes.

Evaluation period

You can install a fully functional version of InterScan MSS for an evaluation period by registering through the Trend Micro website. You will receive an Activation Code that will allow you to access the full functionality of InterScan MSS for a time. After the evaluation period expires, however, most of the program features are disabled.

Upgrading to the full version

If you decide to purchase the product, you do not need to reinstall. Simply purchase InterScan MSS and enter an Activation Code.

1. In the navigation panel, click **Configuration** > **Product Licenses**.

2. Click **Activate** next to IMSS or SPS to open the appropriate product activation page.
3. Type your product Activation Code
4. Click **Activate** to activate the full version of the product.
5. When you return to the Product Licenses screen, the license status of the product you activated will be **Active** and the license counter will show the number of days remaining before your Maintenance Agreement expires.

Trend Micro™ Security Information

Comprehensive security information is available from the Trend Micro free Virus Information Center. The URL is:

`trendmicro.com/vinfo/`

Access Trend Micro™ Security Information to find out about:

- Virus advisories - current news about the top threats, associated risks, and pattern file update that addresses the threat
- Weekly Virus Report - current news about threats that have appeared in the past week
- VIrus map - a description of threats by location worldwide
- Virus Encyclopedia - a compilation of knowledge about all known viruses
- Test files - a test file for testing InterScan VirusWall, and instructions for performing the test

General virus information, including:

- Virus Primer - an introduction to virus terminology and a description of the virus life cycle
- Safe computing guide - a description of safety guidelines to reduce the risk of virus infections
- Risk ratings - a description of how viruses are classified as Very Low, Low, Medium, or High threats to the global IP community
- White papers - that explain such concepts as the real cost of a virus outbreak or how to manage email content security
- Webmaster tools - free virus information updates and tools

- TrendLabs - the ISO 9000-certified virus research and product support center

Technical support

A license to Trend Micro antivirus software usually includes the right to receive pattern file updates and technical support from Trend Micro or an authorized reseller, for one (1) year. Thereafter, you must renew Maintenance on an annual basis at Trend Micro's then-current Maintenance fees to have the right to continue receiving these services.

Contact information

In the U.S., Trend Micro representatives can be reached by phone, fax, or email.

Visit our Web site at:

```
www.trendmicro.com
```

Technical support information

For tech support in the U.S. and Canada, contact us at:

```
support@trendmicro.com
```

For tech support outside the U.S. and Canada, contact us at:

```
www.trendmicro.com/support/
```

Phone numbers

- Our main U.S. phone and fax numbers are:

```
Toll free: +1-800-228-5651 (sales)
Voice: +1-408-257-1500 (main)
Fax: +1-408-257-2003
```

- To reach us outside the U.S., call:

```
+1-408-257-1500 (main)
```

- Our U.S. headquarters are located in Silicon Valley at:

```
Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
```

Knowledge Base

Trend Micro provides Knowledge Base, our online knowledge database.

You can use Knowledge Base, for example, if you are having trouble receiving program file updates or if you are getting an error message. You can search Knowledge Base, using the text of the message, to find out what is causing the problem and how to fix it.

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

To access the Trend Micro Knowledge Base, go to the following Web site:

`kb.trendmicro.com/solutions/`

Appendix A

Reference Information

This appendix contains reference information about InterScan MSS™, including:

- Default directory locations used during mail processing
- Instructions on using InterScan MSS's built-in tokens for additional information in notification messages
- Technical information about how the installation program migrates previous InterScan VirusWall and InterScan eManager™ configuration settings
- A table showing the MIME content-type names used by common Windows email clients and two Web-based email providers

Default directory locations

InterScan MSS uses several directories to process messages, store log files, and quarantine messages. The default locations of these directories appear below.

Processing, retry and postpone queues

The processing queue is where messages are kept pending scanning and final delivery to their destination:

```
/opt/trend/imss/mqueue/
```

The retry queue is where undeliverable messages are kept pending retry:

```
/opt/trend/imss/bmqueue/
```

The postpone queue is where messages are stored temporarily as a result of a postpone filter action:

```
/opt/trend/imss/postpone/
```

To configure these directories, see *Configuring directories* starting on page 3-19.

eManager, virus and program logs

Many modules in InterScan MSS write log information for troubleshooting purposes to the following folder:

```
/opt/trend/imss/logs/
```

For more information, see *Log maintenance* starting on page 3-25.

Default quarantine area

There is one default quarantine area established after program installation. In addition, multiple quarantine directories can be defined in different locations:

```
/opt/trend/imss/queue/quarantine/
```

To change the quarantine directory, see *Managing quarantine areas* starting on page 4-12.

Temporary folder

All application-generated temporary files are stored in the temporary folder:

```
/opt/trend/imss/temp/
```

Note: This directory is not configurable.

Notification pickup folder

All notification messages are put into this folder. InterScan MSS has dedicated threads to pick up messages in this folder and deliver them to a specified SMTP notification server. This server can be configured on the **Configuration > Event Monitoring > Notification** page. See *Notification settings* starting on page 3-21 for more information.

```
/opt/trend/imss/pickup_notify/
```

Note: This directory is not configurable.

Using tokens in notification messages

Notification message tokens

The following tokens can be used in notifications to provide more information about the event that triggered the notification:

- %SENDER%: Message sender
- %RCPTS%: Message recipients
- %SUBJECT%: Message subject
- %DATE&TIME%: Date and time of incident
- %MAILID%: Mail id
- %RULENAME%: Name of the policy that contained the triggered filter
- %FILTERNAME%: The type of filter—either Antivirus Filter, Advanced Content Filter, Message Size Filter, etc.
- %FILENAME%: The name of the attached file.
- %TASKNAME%: The name of the filter that user entered during filter creation
- %GLOBALACTION%: Current action to be taken
- %DETECTED%: Current filter scan result in other task
- %QUARANTINE_PATH%: Quarantine path (if quarantine action performed)
- %QUARANTINE_NAME%: Quarantine name (if quarantine action performed)
- %QUARANTINE_AREA%: Quarantine area (if quarantine action performed)
- %ADDINFO%: Additional information from filter (currently used when the result of the Antivirus Filter is uncertain)
- %CLSNAME%: Name of current filter action
- %DEF_CHARSET%: Default character set of the notification message

Sample message using tokens

For example, suppose the following notification message was configured:

```
The “%FILTERNAME%” filter defined in InterScan MSS has
detected the following message using its “%RULENAME%” rule.
The message’s ID is %MAILID%. The following information
describes the message that may contravene your company’s
policy:

Message sender: %SENDER%
```

```
Message recipients: %RCPTS%

Message subject: “%SUBJECT%”

Incident time: %DATE&TIME%

Per the configuration of your filter’s action, this message
can be reviewed in the “%QUARANTINE_NAME%” quarantine area.
```

A sample notification message in response to a virus event might appear as below:

```
The “Detect Script Viruses” filter defined in InterScan MSS
has detected the following message using its “Catch
LOVELETTER” rule. The message’s ID is 12345-12345-12345-12345.
The following information describes the message that may
contravene your company’s policy:

Message sender: Joe@yahoo.com

Message recipients: Rahul@company.com

Message subject: “Check out the attached Loveletter coming
from me”

Incident time: 10-30-2004, 6:15 PM

Per the configuration of your filter’s action, this message
can be reviewed in the “VirusArea1” quarantine area.
```

Antivirus filter tokens

The following tokens can be used in messages that are inserted into the body of infected email messages:

- %FILENAME%: Filename of the attached file (“noname” when file name cannot be determined)
- %VIRUSNAME%: List that shows all viruses found
- %ACTION%: “Pass”, “clean”, “remove”, or else defined by the process
- %MAXENTITYCOUNT%: String that shows the maximum number of entities that will be scanned, for example “20”. This is configurable on the **Configuration** > **Security** > **Security Settings** screen.

Sample message using tokens

For example, suppose you configured the following message to insert inside an infected message:

```
A file attached to this message, %FILENAME%, was infected with
the “%VIRUSNAME%” computer virus. InterScan MSS has taken the
following action against the message: %ACTION%.
```

In the event a virus was detected, the text that would be inserted into the body of the email message would appear as follows:

```
A file attached to this message, resume.doc, was infected with
the “W97M_MARKER” computer virus. InterScan MSS has taken the
following action against the message: CLEAN.
```

How policies are matched

If the addresses of a message match more than one route, InterScan MSS calculates the priority of the routes to determine which policy (that is, the one with the highest route priority) applies to the message. If two routes (at the same level) have the same priority, we apply the one that has the highest position in the policy hierarchy. For more information about how priority is calculated, see *Priority rules* starting on page A-7.

InterScan MSS uses the best match searching algorithm to traverse the policy tree in level-order, searching the policy tree up and down one level at a time. It will first choose the best match on the top level and then continue searching its child level (if any) until no route matches or a “leaf” is found.

Priority rules

There are two basic rules:

1. A fully qualified address, for example, user@domain.com, has the highest priority and a fully wildcarded address, for example, *, has the lowest priority.
2. The number of qualified terms that an address contains increases the priority. In addition, the significance of the domain versus name, and the sender versus receiver, is evaluated based on the following rules:
   a. An email address’ domain part is more significant than the name part.
   b. Both sender and receiver addresses are of equal importance.

When InterScan MSS analyzes messages, it assigns every email address a weight. It also assigns a weight to every sender and recipient pair (a “route”) by adding the weights of the sender and receiver addresses.

The following table lists the six types of email addresses and their corresponding weights:

	Name part	Domain part	Weight	Example
1	Fully wildcarded		0	*@*, *
2	Qualified	Fully wildcarded	1000	user@*
3	Wildcarded		2000 + #Q #Q: The number of qualified terms in the domain part.	*@*.uk *@*.co.uk *@*.domain.co.uk
4	Qualified	Wildcarded	3000 + #Q	joy@*.uk joy@*.co.uk joy@*.domain.co.uk
5	Wildcarded	Fully qualified	4000	*@domain.co.uk
6	Fully qualified		5000	joy@domain.co.uk

Table A-1. Calculating weights for email addresses

Consider the following examples:

1. The route (**From:** **@trendmicro.com*, *To:* **@**) has precedence over (**From:** *joy@*.com*, **To:** **@**). When the recipient is the same, the weight of **@trendmicro.com* is higher than *joy@*.com* because the domain is more significant than the name.
2. The incoming route (**From:** **@**, **To:** **@trendmicro.com*) has the same precedence as outgoing route (**From:** **@trendmicro.com*, **To:** **@**) because the sender and receiver addresses are of equal importance.
3. The route (**From:** **@trendmicro.com*, **To:** **@*.com*) has precedence over (**From:** *joy@trendmicro.com*, **To:** *joy@**). This is because the weight of the sender and receiver pair of the former route is (4000, 2001), but the latter is (5000, 1000).
4. The route (**From:** **@*.co.uk*, **To:** **@*.co.uk*) has precedence over (**From:** **@*.domain.co.uk*, **To:** **@**). This is because the weight of the sender and receiver pair of the former route is (2002, 2002), but the latter's is (2003, 0).

MIME Content-types used by email clients

Windows Clients

	Outlook Express 6	Netscape Mail 6.1	Eudora 5.1
Jpeg/Jpg	Application/octet-stream	Image/jpeg	
Gif	Image/gif		
Bmp	Image/bmp		Application/octet-stream
Tif/Tiff	Image/tiff		
Wav	Audio/wav		Audio/microsoft-wave
Mp3	Audio/mpeg	Audio/x-mpeg	Audio/mpeg
Midi	Audio/mid		
Mpeg	Video/mpeg		
Avi	Video/x-msvideo		Video/avi
Asf	Video/x-ms-asf		Application/octet-stream
Wmv	Video/x-ms-wmv		
Quicktime	Video/quicktime		
Rtf	Application/msword		Application/rtf
Pdf	Application/pdf		
Zip	Application/x-zip-compressed		Application/zip
Msword	Application/msword		
Msexcel	Application/vnd.ms-excel		Application/octet-stream
Mspowerpoint	Application/vnd.ms-powerpoint		Application/octet-stream

Table A-2. MIME Content types by email clients

Web-based email providers

	MSN Hotmail (Web-based)	Yahoo Mail (Web-based)
Jpeg/Jpg	Image/pjpeg	
Gif	Image/gif	
Bmp	Image/bmp	
Tif/Tiff	Application/octet-stream	Image/tiff
Wav	Audio/wav	
Mp3	Audio/x-mpeg	
Midi	Audio/mid	
Mpeg	Video/mpeg	
Avi	Video/avi	
Asf	Video/x-ms-asf	
Wmv	Video/x-ms-wmv	
Quicktime	Video/quicktime	
Rtf	text/richtext	
Pdf	Application/pdf	
Zip	Application/x-zip-compressed	
Msword	Application/msword	
Msexcel	Application/vnd.ms-excel	
Mspowerpoint	Application/vnd.ms-powerpoint	

Table A-3. MIME Content types by web-based email providers

InterScan™ Messaging Security Suite Daemons

The following information explains the various InterScan MSS daemons, their purpose, and the relationships between them.

Web Interface-Related Daemons

The area within the dotted lines at the top right are three daemons that are part of the installation package:

- APACHE server
- TOMCAT server
- Trend CCGI

TMI helps the UI communicate with the Web server and ensures that this channel is secure.

The following is the process list for the UI:

root 9061 1 0 Nov 06 ? 0:37 /opt/trend/imss/bin/aphost

root 8819 1 0 Nov 06 pts/18 0:00 /opt/trend/imss/TMI/CM

root 8866 8819 0 Nov 06 pts/18 0:00 /opt/trend/imss/TMI/LWDMServer

root 8822 8819 0 Nov 06 pts/18 0:09 mrf

imss 8998 8988 0 Nov 06 ? 0:01 /opt/trend/imss/common/apache/bin/httpd -d /opt/trend/imss/common/apache -DSSL

imss 18067 8988 0 Nov 12 ? 0:01 /opt/trend/imss/common/apache/bin/httpd -d /opt/trend/imss/common/apache -DSSL

imss 3133 8988 0 Nov 07 ? 0:01 /opt/trend/imss/common/apache/bin/httpd -d /opt/trend/imss/common/apache -DSSL

imss 3129 8988 0 Nov 07 ? 0:01 /opt/trend/imss/common/apache/bin/httpd -d /opt/trend/imss/common/apache -DSSL

imss 8988 1 0 Nov 06 ? 0:00 /opt/trend/imss/common/apache/bin/httpd -d /opt/trend/imss/common/apache -DSSL

imss 8997 8988 0 Nov 06 ? 0:01 /opt/trend/imss/common/apache/bin/httpd -d /opt/trend/imss/common/apache –DSSL

imss 8893 1 0 Nov 06 pts/18 0:33 /opt/trend/imss/common/jre/bin/../bin/sparc/native_threads/java -Dtomcat.home=/

Scanning Daemon

The following figure is a detailed view of the scanning daemon.

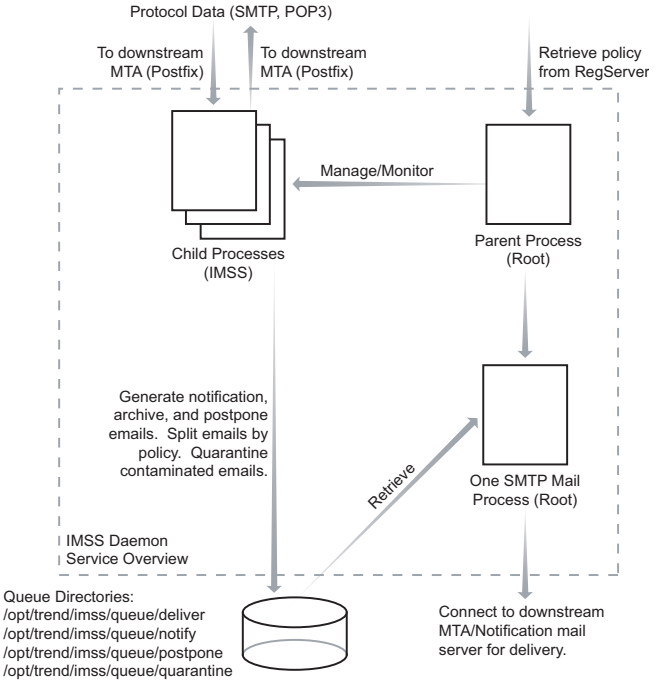


FIGURE 1-4. Scanning Daemon Overview

This daemon is responsible for SMTP and POP3 content scanning.

- imss 29293 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- imss 29296 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd

- imss 29294 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- imss 29299 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- imss 29300 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- imss 29295 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- root 29292 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- imss 29302 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- root 29291 1 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- imss 29297 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- imss 29301 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd
- imss 29298 29291 0 12:25:34 ? 0:00 /opt/trend/imss/bin/imssd

The parent process (29291) is running as root. The first child process (29292) is also running as root, but it is responsible for delivering extra messages, such as notification messages, split messages, and postpone messages. The other child processes (29293 – 29302) are running as low-privilege user “imss” for security concern.

Regserver Daemon

This daemon keeps the policies. There is only one process associated with this daemon, and it can read and write to the XML file shown above.

- root 16614 1 0 Nov 12 ? 0:29 /opt/trend/imss/bin/regserver /opt/trend/imss/config/imss.ini

System Monitor Watchdog Daemon

This daemon monitors the UI, the aphost daemon, and other system resources.

- root 5911 1 0 18:43:35 ? 0:00 /opt/trend/imss/bin/imsssysmon

Content Scanning Flow Chart

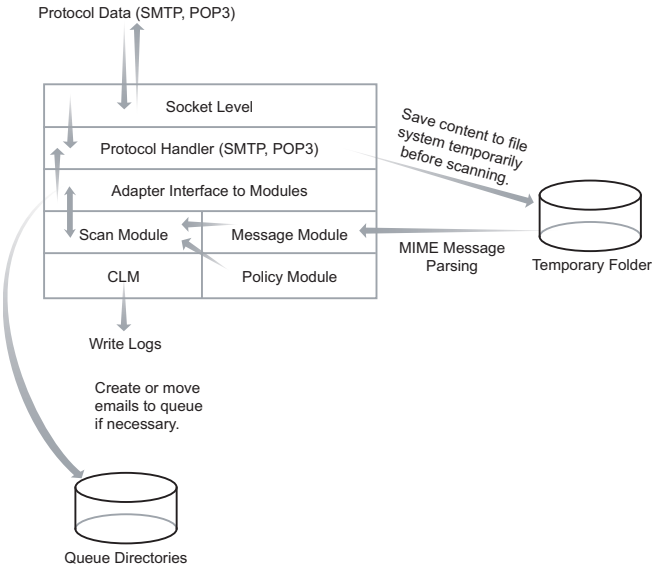


FIGURE A-5. Content Scanning Data Flow

This figure illustrates the flow that messages take during scanning.

1. At the socket level, InterScan MSS receives protocol data.
2. The SMTP and POP3 proxies receive this data.
3. InterScan MSS temporarily saves this data before scanning it.
4. Then it passes the content to the scanning module. Here, the Policy and Message modules apply the relevant policies and scan the contents.
5. The content is passed to the adaptor interface to the modules and up to through the Protocol Handler and to the Socket Level, where it is sent to the recipient.

InterScan MSS Daemon Relationships

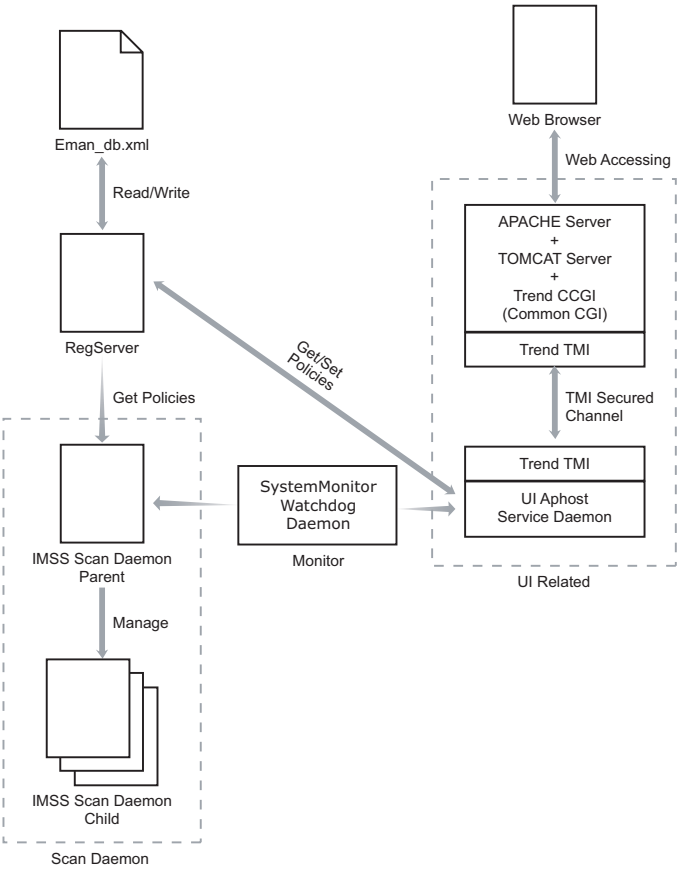


FIGURE A-6. Daemon Relationships

Figure A-6 maps the relationship between the daemons that are associated with InterScan MSS.

Uninstalling Postfix

If during installation, you installed Postfix, but would now like to remove it from your system, this appendix shows you this process.

WARNING! *This is not an officially recommended procedure.*

```
postfix stop
rm -rf /usr/libexec/postfix
rm -rf /etc/postfix
rm /usr/sbin/post*
mv /usr/lib/sendmail.OFF /usr/lib/sendmail
```

Appendix B

AMON™ Setup for InterScan™ MSS

InterScan MSS provides virus and content scanning capabilities for inbound and outbound mail to the network environment. By integrating with the Check Point™ environment by using AMON (Application Monitoring API) in OPSEC™ (the OPen Platform for Security), InterScan MSS reports scanning statistics to the Check Point System Status Viewer. These include the number of discovered and cleaned viruses, total email and file-specific processing volume, number of SMTP sessions open, bounced message quantity, scan queue size and deliver queue size, and so on.

AMON enables network applications to report their status to the Check Point Management server. Status information is available through the Check Point Status Monitoring application.

For additional information on Check Point and OPSEC, see:

```
http://www.checkpoint.com/index.html
```

For additional information on AMON, see:

```
http://www.opsec.com/intro/sdkds.html#amon
```

Overview

The topology of the AMON server and client is that the server waits for the client's request, produces replies, and sends them back to their initiator.

InterScan MSS provides a stand-alone AMON server program and amon_server to coordinate the information. Another adaptor DLL, amonadaptordll.dll (pre-defined in isntmtp.ini) invokes this program.

Setting up the InterScan MSS AMON application

Check Point™ Next Generation FireWall-1® and InterScan MSS do not have to be on the same machine, but they do have to be able to communicate.

1. To set up the InterScan MSS AMON application, you need to get the following files from the AMON folder in the setup package:
   - amon.conf

     Place this file in `<install directory>/imss/opsec/bin`.
   - schema.txt

     Place this file in the same directory as amon_import.exe, which is the Check

     Point program located on the FW-1/VPN-1 management station and will be in `$FWDIR/bin`, for example:

     `c:\winnt\FW1\5.0\bin`
2. In the **Check Point Policy Editor** screen, create a new OPSEC™ application.

   Check that the amon_import file is in the following default location: c\winnt\FW1\5.0\bin.
3. Import InterScan MSS's private schema file by running amon_import schema.txt. We recommend that you place schema.txt in the same directory as amon_import. Use amon_import to import your schema file.
4. Restart the FireWall-1 service. After a successful import and restart, you should see the new default identifier, **InterScan_MSS** when you click the **AMON Options** tab in the **OPSEC Application Properties** window.

5. Open the newly created OPSEC application object. Click the **General** tab. Enter the appropriate information in the fields at the top and select **AMON** under **Server Entities** and click **Communication**.

Note: To make the **AMON Options** tab visible, you have to first select **AMON** under **Server Entities**.

---

6. In the **OPSEC Application Properties** screen, click the **AMON Options** tab. Using the **Service** pull-down menu, select the service. (The default service is **FW1_amon**, which is port 18193.) Using the **AMON identifier** pull-down menu, select **InterScan_MSS**. Click **OK**.

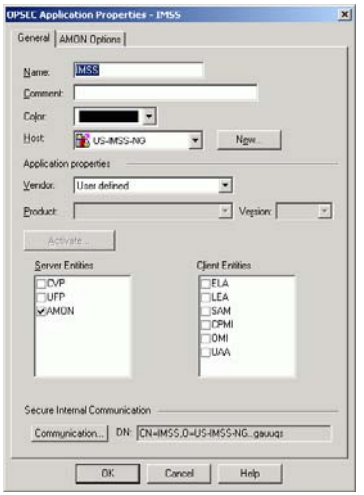


FIGURE C-3. OPSEC™ application properties screen

7. In the **Communication** screen, enter an activation key in **Activation Key**; re-enter it in **Confirm Activation Key** and click **Initialize**. (The activation key is the one used in opsec_pull_cert.)
8. Install your policy.

9. Obtain the opsec_pull_cert.exe from the setup package's amon folder and run this file on the machine that has InterScan MSS. Running opsec_pull_cert.exe generates the p12 file.

   To establish a "trust" internal communication, run **`opsec_pull_Cert -h`** (host) **`-n`** (amon_object) **`-p password`**. Host is the machine IP with the management console of FireWall-1 Next Generation, amon_object is the name of the newly created OPSEC application, and password is the password at initialization.

10. Return to the **Communication** screen to see if **trust established** appears in the **Trust state** field.

11. Open the amon.conf file and make sure the opsec_sic_name is exactly the same as the DN of the OPSEC object you just created. (Ensure that the proper case and quotes are used). To avoid mistakes, we recommend that you cut and paste the DN into the amon.conf file.

    Quotes are required if spaces are inserted into the opsec_sic_name. Improper case in an object (i.e. FW1object vs. FW1OBJECT) causes sic failure.

Note: Make sure that you put the amon.conf file in `/imss/opsec/bin`, which is also the location for the amonmainexe.exe file.

---

12. In the amon.conf file, check that:

    - The opsec_sslca_file is pointing to the correct location of the opsec.p12 file. By default, we use "sscla" authorization type.
    - You are using the correct port number and IP address. By default, AMON uses port 18193. If you want to use a different port, you need to modify the service used by the OPSEC application. The amon_server IP should be the machine running InterScan MSS.

    If you make any changes to the amon.conf file, restart the Trend Micro InterScan Messaging Security Suite system monitor service.

13. Verify the status of this connection in the **Check Point Status Manager** screen. If the connection has been made, under **Status**, you will see the application name (Trend Micro InterScan Messaging Security Suite for SMTP) with a green check mark and **OK**.

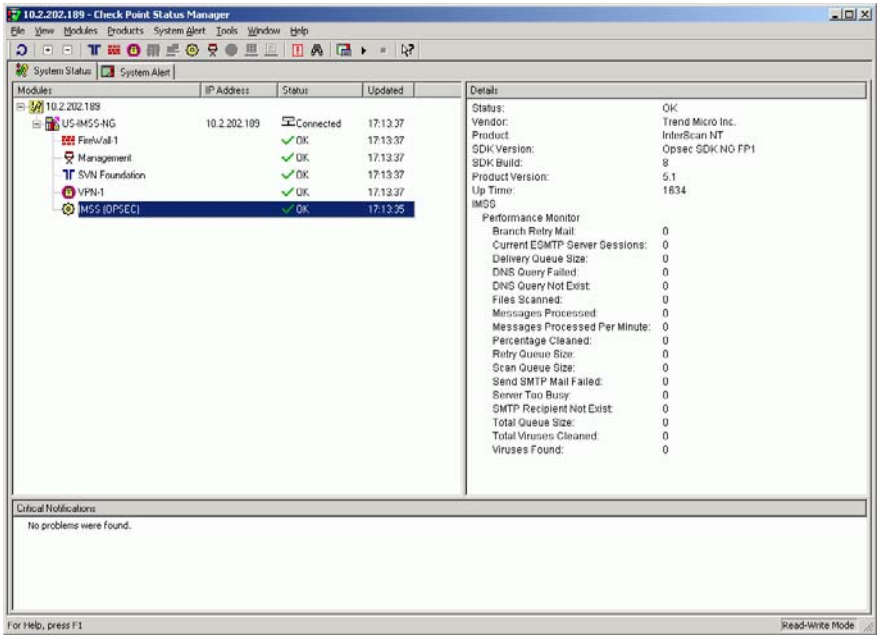


FIGURE C-4. Check Point™ Status Manager screen

Verify that the AMON server is working

From the Check Point Status Manager screen

To verify that the AMON server is working, open the **Check Point Status Manage**r screen and send messages through InterScan MSS. If the AMON server is working, the counters listed in the **Details** frame will increment.

From the ps command on the AMON Server Side

You can also verify that the AMON server is working by using the `ps` command on the AMON server side:

Type `ps -elf | grep amon_server` on the console to see whether the AMON server is running.

Troubleshooting

If you are having problems, check that:

- The amon.conf file is correctly configured and is in the same directory as the amonmainexe.exe file.
- You have successfully imported the schema.txt file.
- Using the **AMON identifier** pull-down menu in the **OPSEC Application Properties** screen, you selected **InterScan_MSS**.
- You installed the policy.
- FireWall-1 can communicate with the machine on which InterScan MSS is installed.

InterScan MSS data model

For the data model, we use the same object ID (OID) tree for AMON and SNMP. The numbers below are the leaves of the OID tree.

In amonmainexe.exe, two category are provided:

- Performance monitor
- OPSEC-defined generic status fields

Performance Monitor information

This InterScan MSS proprietary information will be a prefix to the Check Point OID, 1.3.6.1.4.1.6101.23.1.

The OID explanation is:

- Iso (1)
- Org (3)
- Dod (6)
- Internet (1)
- Private (4)
- Enterprises (1)
- Trend Micro (6101)
- InterScan VirusWall NT(23)
- AMON sub-tree (1)

For example, 1.3.6.1.4.1.6101.23.1.4 may be used for delivery queue size. Detailed information is listed in the table below.

Counter name OID value type description

Counter Name	OID	Value Type	Description
FileScanned	1	Integer	This is the total number of files that have been scanned for viruses since the program started.
VirusesFound	2	Integer	This is the total number of virus-infected files found since the program started.
ScanQueueSize	3	Integer	This is the current number of messages waiting to be scanned.
DeliveryQueueSize	4	Integer	This is the current number of messages waiting to be delivered.
RetryQueueSize	5	Integer	This is the current number of messages waiting to be delivered. Messages were put into the Retry queue if they could not be delivered.
TotalQueueSize	6	Integer	This is the current number of messages waiting to be delivered. This is the sum of the Scan, Deliver and Retry queues.
MessageProcessed	7	Integer	This is the total number of messages that have been processed since the program was started.
TotalVirusesCleaned	8	Integer	This is the total number of virus-infected files that have been cleaned since the program was started.

Counter Name	OID	Value Type	Description
MessagesProcessed-PerMinute	9	Integer	This is the number of messages processed per minute since the program was started.
PercentageCleaned	10	Integer	This is the percentage of virus infected files that were cleanable when action on viruses is to auto-clean.
DnsQueryFailed	11	Integer	This is the total number of DNS query errors that have been found since the program started.
DnsQueryNotExist	12	Integer	This is the total number of “DNS query domain not exist” errors that have been found since the program was started.
SmtpRcptNotExist	13	Integer	This is the total number of “sendmail to recipient not exist” errors that have been found since the program started.
SendMailSmtpFailed	14	Integer	This is the total number of “send SMTP mail” errors that have been found since the program started.
BranchRetryMail	15	Integer	This is the total number of retry messages that have been branched since the program started.
ServerTooBusy	16	Integer	This is the total number of “Service not available, closing transmission channel” since the program started.

Counter Name	OID	Value Type	Description
CurrentESMTPServ-erSessions	17	Integer	This is the total number of ESMTP server sessions in progress.

Some generic status fields defined by OPSEC

These generic status fields show some basic information of each product, such as the product name, program status. Their field prefix is 1.3.6.1.4.1.2620.2.1.1. The detail information description list in the table below.

For example, 1.3.6.1.4.1.2620.2.1.1.4 means product name—InterScan MSS.

Name	OID	Value Type	OPSEC VT Type	Description
statusOK	1	Integer	OPSEC_VT_132BT	0, if the status of the application is OK; otherwise, non-zero.
statusDescription	2	String	OPSEC_VT_STRING	Text description of the status of the application.
opsecVendor	3	String	OPSEC_VT_STRING	Text description of the status of the application.
opsecProduct	4	String	OPSEC_VT_STRING	The product name.
opsecProductVersion	5	String	OPSEC_VT_STRING	The product version.
opsecSdkVersion	6	String	OPSEC_VT_STRING	The OPSEC SDK Version.
opsecSdkBuildNumber	7	Integer	OPSEC_VT_U132BIT	OPSEC SDK build number.
opsecAppUpTime	8	Integer	OPSEC_VT_U132BIT	The number of the sessions when the content was safe.

Appendix C

Installing the Trend Micro™ Control Manager™ Agent

Control Manager delivers Outbreak Prevention Services to Trend Micro products, including InterScan MSS, to address emerging virus threats prior to pattern file updates. With single point-of-contact administration, monitoring, and deployment, corporations can more effectively manage their antivirus and content security strategies enterprise-wide. Control Manager provides a framework for the Outbreak Prevention Service that assists in collectively addressing the antivirus concerns of the business.

The Control Manager server communicates with its managed products through applications called agents. InterScan MSS uses a Control Manager agent that is specifically designed for it. Through Control Manager, you can remotely configure groups of servers to perform the same tasks and use the same configuration settings. If you have a large network, Control Manager can help you reduce the time you spend configuring your servers.

This appendix explains how to install (and remove) the Control Manager agent for InterScan MSS.

Note: For IMSS 5.7, the Control Manager configuration replication function will not replicate database.ini file, nor the scanagent.ini. If these files have been altered, you must manually copy them between servers.

Agent installation program components

The agent package is composed of two parts:

- The Communicator
- The agent program

The Communicator is the managed product-side component of TMI — the communications backbone of the Control Manager network. Control Manager agents have their own local Communicator, which is shared by all the agents on that server. Although there can be as many agents on a server as there are managed products, only one Communicator is required for each server. TMI uses the same encryption key and message routing settings for all agents installed on a server.

The Communicator can be upgraded and released independently, without upgrading the agent.

Control Manager agents do the following:

- Receive command inputs from the Control Manager server and apply them to the managed product
- Collect logs from the product and report them to the Control Manager server

Installing the agent

You can only install the agent from the client server, it cannot be installed from the TMCM server.

To install the agent:

1. Open a console window and switch to the install package path.
2. If you didn't install the Control Manager agent during your original IMSS installation, you can type command `./isinst -tmcmagent` to install this component.
3. Provide the entity name; the name displayed on the Product Directory for example, `suse8`.
4. Provide a CM server account which you want to register the agent. For example you could specify `root`.

Note: When installing agents, we recommend that you use the root account.

---

5. Provide the CM server information:
   - IP address or hostname
   - Port. The default port number is 80, If your CM server's configuration is not the default port, e.g, 8080, you should provide the port information.
6. After installation, you will see the entity `suse8` from the CM server.
7. Click the entity to view its status.

Note: You can install the component during the initial installation of IMSS. You will be prompted whether to install the agent. Type `yes` and follow the steps outlined above.

Removing the agent

To remove the agent, you can use the command `./isinst -uninstallagent`,

If you want to remove this component, ensure that there is connectivity between the agent and Trend Micro Control Manager server, because the agent will unregister itself from Control Manager before removing the agent component.

1. Open a console window, switch to the install package's path.
2. Type `./isinst -uninstallagent`.

Index

T

U

V

W