TREND MICRO™

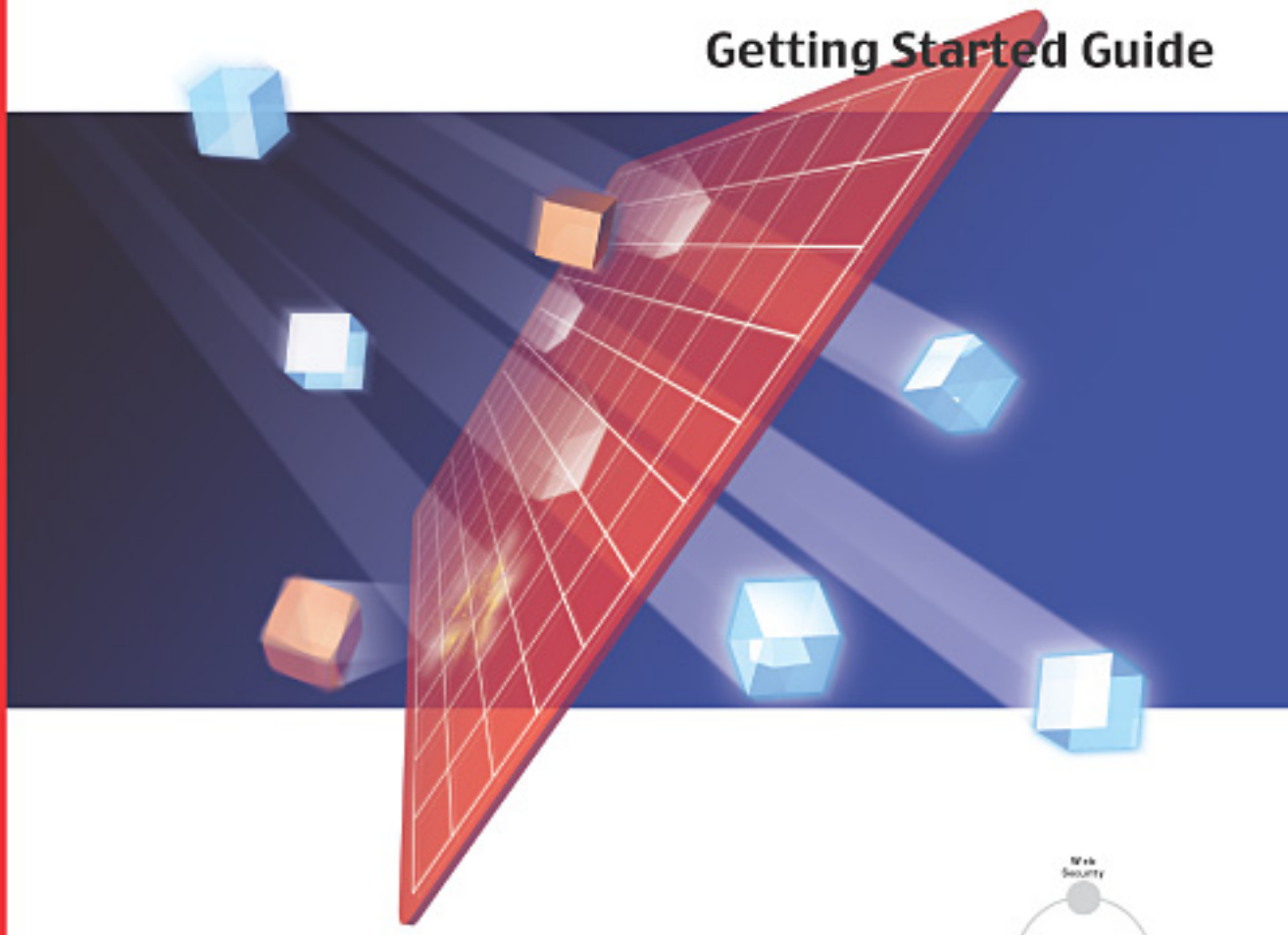
InterScan™ 5

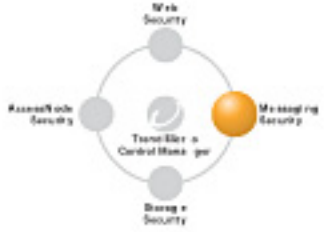
Messaging Security Suite

Antivirus and Content Security for the Messaging Gateway

for Microsoft™ Windows™ 2000/Windows NT™

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: August 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 -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

Index

Figures

Tables

Chapter 1

Introducing InterScan™ MSS

InterScan™ Messaging Security Suite (InterScan MSS) 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

Virus detection is performed using Trend Micro's scan engine and a process called pattern matching. The scan engine uses a virus pattern to compare files travelling through your gateway with binary patterns of known viruses. If a virus is detected, the scan engine attempts to clean the file by removing the virus code. Trend Micro releases new virus pattern files as new viruses are detected.

In addition, Microsoft® Office® files are scanned with Trend Micro's 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. Email is an indispensable business tool which must be managed properly to ensure its productive use. Content that you deem inappropriate, such as personal communication, large attachments, and so on, can be blocked or deferred effectively using InterScan MSS.

Spam filtering

With the integration of SPS technology (licensed separately), InterScan MSS provides spam filtering capabilities, using rules to identify spam. Integration with Trend Micro IP-Filtering (licensed separately) allows IMSS to block spam before it enters your network.

The Trend Micro End-user Quarantine solution, which provides web-based access to spam messages, provides additional flexibility for spam management. For more information about EUQ, see Working with the Centralized Spam Reporting and Web-based Quarantine starting on page 8-1.

Protection against other email threats

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

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 are allowed to pass through 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. When inappropriate messages originate from a company's mail server, the company's reputation can be damaged, 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 that messages containing inappropriate or confidential material will be allowed 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 they become a problem.

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 than 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.

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, a IP-level spam filtering product (licensed separately), which blocks spam 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.

End User Quarantine

The End User Quarantine (EUQ) feature, for users who have licensed Trend Micro Spam Prevention Solution (SPS), provides Web-based end user access to spam quarantines. EUQ requires a database and a connection to LDAP 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.

InterScan MSS main benefits

InterScan™ Messaging Security Suite includes the following benefits:

- Advanced Performance: InterScan MSS enhanced MTA, MDA and 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: Email routing can be flexibly configured based on recipient domains.
- Integration with Trend Micro™ Control Manager™: Outbreak Prevention Services are delivered through Trend Micro Control Manager as part of Outbreak Commander™. When a new email-borne virus is detected, Trend Labs issues a policy that uses the advanced content filters in InterScan MSS to block messages by identifying suspicious characteristics in these message. 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 they are retrieved by clients in your network.
- Policy-based Management: Multiple virus and content filtering policies can be defined on a single InterScan MSS server to enforce your company's email usage guidelines. Policies can be defined 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 spam filtering: The detection technology used by Spam Prevention Solution (SPS) is based on sophisticated content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high performance, real-time detection that is highly adaptable, even as spammers change their techniques.
- 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 that is applied to members of your organization. Different policies can be configured 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 the InterScan MSS 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 a message is received by the InterScan MSS server, the sender and recipient addresses are analyzed to determine which policies apply. The filters configured for the applicable policies are applied and trigger a filter result. For each filter result, there is 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 policies are applied 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 scenarios
- Information for installing Web EUQ and IP Filtering
- Upgrading from previous versions
- Minimum system requirements
- Pre-installation checklist
- Information required to install InterScan MSS
- Opening the InterScan MSS console
- Configuring InterScan MSS after installation
- Encrypting console-server communication using SSL
- Upgrading from the evaluation period
- Uninstalling and porting settings to a new server

Choosing your installation server

For optimal performance, install InterScan MSS on a dedicated machine with a configuration similar to your existing SMTP server.

Apart from meeting the system requirements (see *Recommended system requirements* starting on page 2-12) 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 scenarios

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 by using multiple smart hosts or specific DNS servers.

Installing before the firewall/no firewall

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

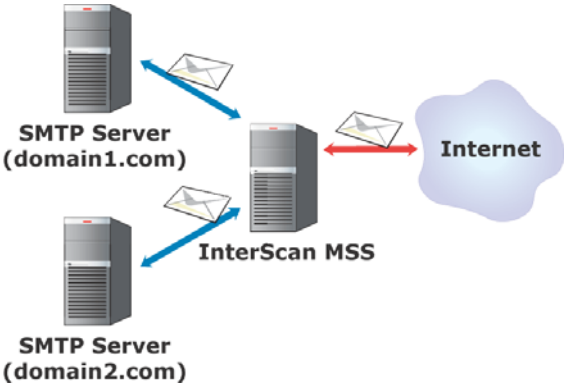


FIGURE 2-1. Installation topology: no firewall

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

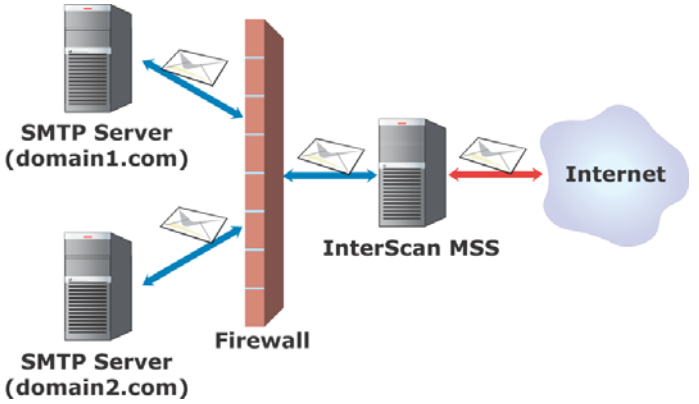


FIGURE 2-2. Installation topology: before the firewall

Incoming traffic

- InterScan MSS should be the first server to receive incoming email. Configure the MX records on the DNS servers that currently reference your SMTP gateway or firewall to reference the address of the InterScan MSS server(s).
- Configure the **Relay Control** settings to only allow relay for local domains.

Outgoing traffic

- If there is no firewall, configure SMTP gateways to route all outgoing email to InterScan MSS.
- If there is a firewall, configure the firewall (proxy-based) to route all outbound messages to InterScan MSS, so that:
  - Outgoing SMTP email can only go to the InterScan MSS server(s).
  - Incoming SMTP email can only come from the InterScan MSS server(s).
- Configure InterScan MSS to allow internal SMTP gateways to relay, through InterScan MSS, to any domain.

Installing behind a firewall

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

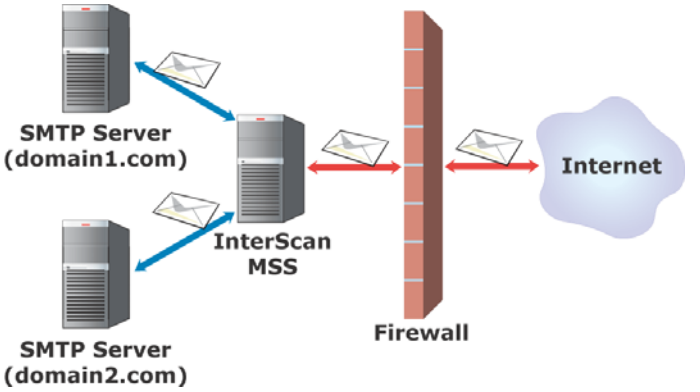


FIGURE 2-3. Installation scenario: behind a firewall

Incoming traffic

- Configure your proxy-based firewall, so:
  - Outgoing SMTP email can only go to the InterScan MSS server(s).
  - Incoming SMTP email can only come from the InterScan MSS server(s).
- Configure your packet-based firewall. Change the MX records on the DNS server that currently reference your SMTP gateway to reference the address of the server hosting InterScan MSS. Point your MX records to InterScan MSS or the firewall, if it is configured to manage a secure subnet.
- Configure InterScan MSS to route email destined to your local domain(s) to the SMTP gateway or your internal mail server (Exchange IMS).
- Configure relay restriction to only relay for local domain(s).

Outgoing traffic

- Configure all internal SMTP gateways to forward outgoing mail to the InterScan MSS server.
- If you are replacing your SMTP gateway with InterScan MSS, configure your internal mail server (for example, Exchange IMS) to forward outgoing email to the InterScan MSS server.

- Configure InterScan MSS to route all outgoing email (to domains other than the local domains), to the firewall, or deliver this email by using an external DNS server.
- Configure InterScan MSS to allow internal SMTP gateways to relay, by using InterScan MSS, to any domain.

Installing on a former SMTP gateway

The following figure illustrates how InterScan MSS can be installed on the same server that formerly hosted your SMTP gateway:

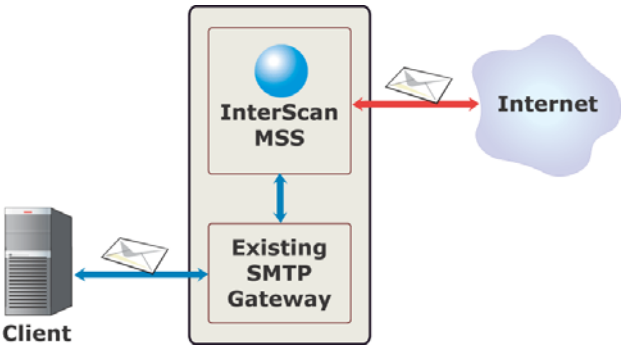


FIGURE 2-4. Installation scenario: on a former SMTP gateway

On the SMTP gateway:

- Allocate a new TCP/IP port to route SMTP mail in the gateway. It must be a port that is not being used by any other services.
- Configure the existing SMTP gateway to bind to the newly-allocated port, which frees port 25.
- Install InterScan MSS—and it 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 InterScan MSS to route all outgoing email (those messages destined to domains that are not local) to the firewall or deliver using an external DNS server.

In the DMZ

The following figure shows how InterScan MSS can be installed in the DMZ:

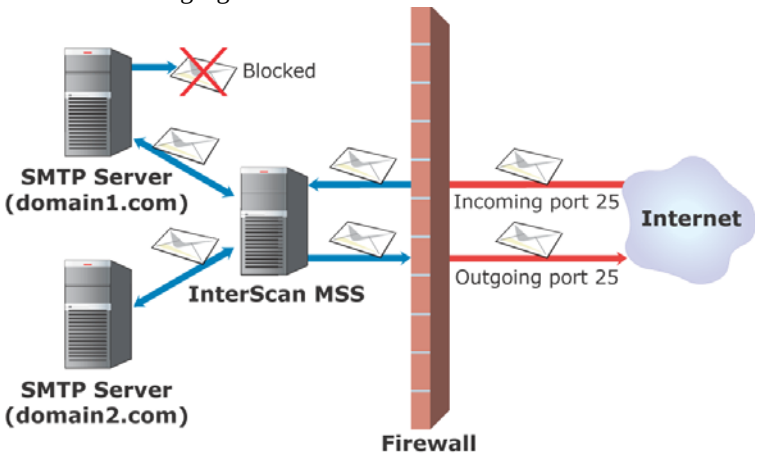


FIGURE 2-5. Installation scenario: in the DMZ

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. Change the mail exchange (MX) records on the DNS server that currently reference your SMTP gateway to reference the address of the server hosting InterScan MSS.
- Configure InterScan MSS to route email destined to your local domain(s) to the SMTP gateway or your internal mail server (that is, Exchange IMS).

Outgoing traffic

- Configure InterScan MSS to route all outgoing email (destined to other than the local domains) to the firewall or deliver by using an external DNS server.
- Configure all internal SMTP gateways to forward outgoing mail to the InterScan MSS server.
- Configure InterScan MSS to allow internal SMTP gateways to relay, through InterScan MSS, to any domain.

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 IMSS, your network topology must be configured so that no address modification occurs between the edge of your network and that connection to IMSS.

Note: This means that any firewall between IMSS 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.

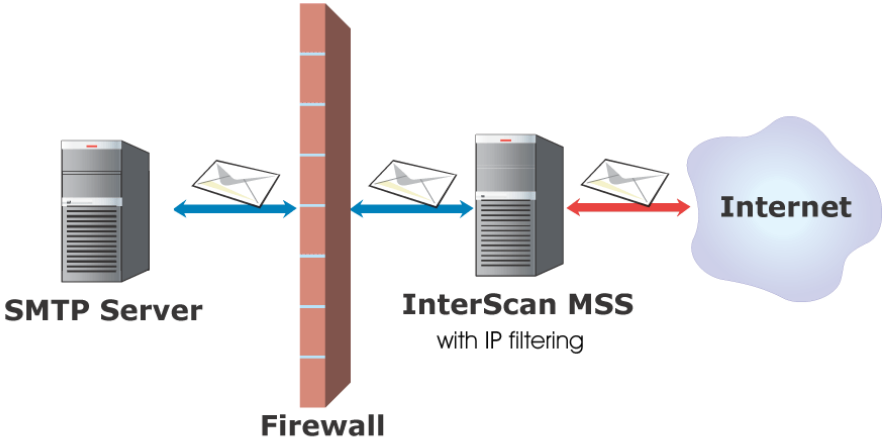


FIGURE 2-6. Installation of IMSS configured for IP filtering

Deploying InterScan MSS with 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.

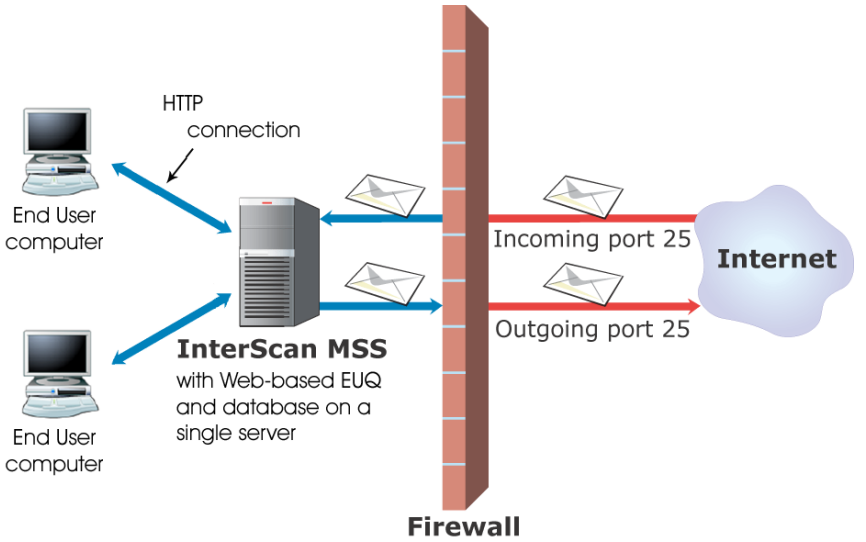


FIGURE 2-7. Installation of IMSS, Web-based EUQ, and database on a single server

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.

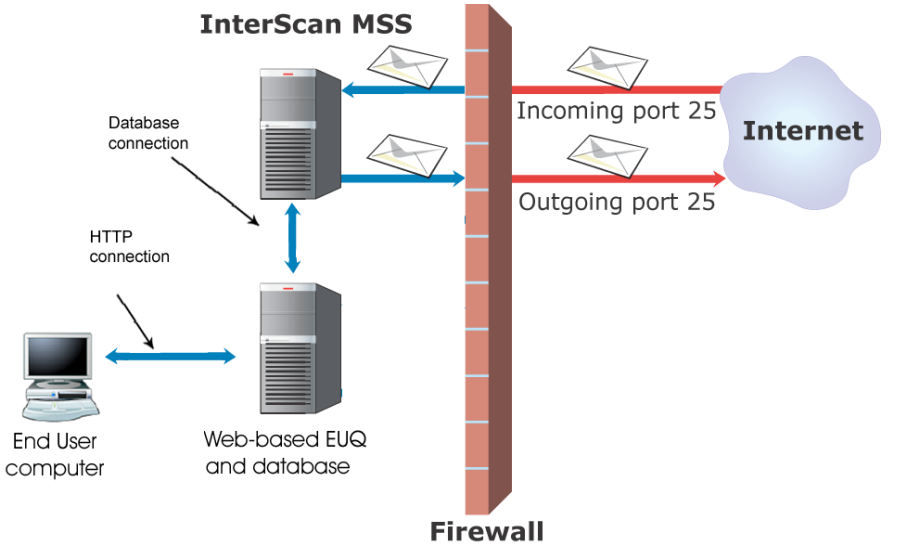


FIGURE 2-8. Installation of IMSS on one server and Web-based EUQ and database on a separate server

Upgrading from previous versions

The InterScan MSS installation program can automatically upgrade from versions 5.1 or 5.5 of InterScan MSS. If the installation program detects either of these versions it can:

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

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 5.5 over an existing installation.

Once you have completed migration, you will need to activate InterScan MSS. While settings from your previous installation will be saved, when you activate InterScan MSS any eManager filters you have configured will automatically be set to Inactive. Use the Policy Manager to reactivate them. For more information on activating InterScan MSS, see *Activating Trend Micro Antivirus and eManager, and the Spam Prevention Solution (SPS)* starting on page 2-25.

Configuration file backup

When installing IMSS on a computer that already has InterScan MSS installed, your customized settings from the previous install are automatically backed up to the \IMSS_RILOG directory on the root drive.

If the target server has a copy of InterScan MSS 5.x, then the following files are backed up:

- isntsmtp.ini
- domaintable.ini
- Tmlogflag.ini
- localdomain.dat
- conn_restrict.dat
- rely_restrict.dat
- vaspi32.dll

These settings are migrated to your new software installation, and backup copies are created in the \IMSS_RILOG directory on the root drive. For additional information on backup and data replication, see *Backing up and replicating data* starting on page 2-29.

Recommended system requirements

- Intel Pentium® III 1GHz or above
- 1GB RAM
- At least 500MB disk space for mail storage

Note: To install InterScan MSS, share C$ or D$ (depending on the target drive) on the target server.

Minimum system requirements

The following hardware and software are required for the server where InterScan MSS will be installed.

Hardware

- Intel™ Pentium™ III processor 800MHz (or equivalent)
- 256MB memory
- 300MB free hard disk space on the directory when InterScan MSS is installed
- 150MB free hard disk space on the system drive where Microsoft® Windows® is installed

Note: The InterScan MSS installation program checks the free disk space on the system and target drives. If your server lacks the minimum disk space, the installation process will not be completed.

Software

- Windows 2003 Server, Windows 2000 Server/Advanced Server with Service Pack 4 or above (preferred) or Windows NT 4 Server (with Service Pack 6A)
- Microsoft® Internet Information Server® (IIS) 4.0 or above to host the InterScan MSS Web console
- Microsoft® Internet Explorer® 5.5 or above (Netscape™ Navigator™ is not supported)

Note: To install InterScan MSS, share C$ or D$ (depending on the target drive) on the target server.

Information required for installation

You need the following information when running the installation program:

- IP address and port number of the SMTP server that currently handles your mail
- IP address and port number of SMTP server to send notification email messages

Note: Do not specify the InterScan MSS machine as your notification server. If you do this, in the event of a malfunction, you cannot receive notification messages from the System Monitor.

- Administrator's email address to receive notifications
- The mail domain name(s) of the server that processes messages for your network (as shown in your DNS server's MX record)
- The machine name of the server where you want to install InterScan MSS
- An administrator credential (user name and password) with local or domain administrative rights to the server where you want to install InterScan MSS.

Note: To encrypt communication between the Web-based management console and the InterScan MSS server using SSL, before starting the installation program, see *Viewing the management console using SSL* on page 2-28.

Installing InterScan Messaging Security Suite

Start the installation program by running Setup.exe from a server or workstation on your network. If you have downloaded the InterScan MSS package from the Internet as a single compressed file, decompress the package to a folder. Be sure that you preserve the folder structure that existed in the compressed file.

Internet Explorer, the Microsoft® management console®, and MMC-related programs may interfere with the installation. Close all instances of these programs on both the target server and the machine from which you are running the remote installation. We recommend temporarily closing all programs on the target server.

Beginning the installation process

1. Run setup.exe. Click **Next** in the **Welcome** screen.
2. Read the software license agreement and signify your agreement by clicking **Yes**.
3. Select the **Install InterScan Messaging Security Suite** option and click **Next**.

Configuring your InterScan MSS installation

Once the installation process begins, you will select whether you need to migrate settings from a previous version, choose which mail protocols to scan, select delivery options, and configure other InterScan™ Messaging Security Suite options.

1. To migrate configuration settings from a previous version of Trend Micro's InterScan MSS, select **Migrate Previous Version Settings**. When you do this, InterScan MSS migrates all the previous settings from your current installation of IMSS.

   The second option on this screen is **Detect and Uninstall the older version of IMSS**. If you select this option, the current installation of InterScan Messaging Security Suite is removed completely.
2. Select whether you want to enable **SMTP Server** or **POP3 Proxy**. We recommend that you select both options. Click **Next.**

   By selecting both options, you allow InterScan MSS to listen for incoming mail on both services. Two benefits of disabling the POP3 adaptor are added security and reduced resource usage.

3. Indicate how you want messages to be delivered after they pass through the InterScan MSS server—forward them to a downstream SMTP server or resolve the addresses using a DNS server. (This step applies only to SMTP messages.) Click **Next**.

   To process messages by forwarding them to an SMTP server, enter this server's IP address and the port of the original SMTP server.

   If you are installing InterScan MSS on the server where your SMTP server is installed, enter the localhost. In this case, the SMTP server should not use port 25. You can also choose to have destination addresses resolved through a DNS server. If you do not specify an IP address, DNS is used to deliver the information. Click **OK** in the pop-up window.

Note: Regardless of whether it is an inbound or outbound message, InterScan MSS's message delivery is based on the domain.

---

4. Enter the SMTP server that will be used to send notification messages. If there are potential problems with the software's operation, or if message detection is stopped by the virus or eManager filters, InterScan MSS can send email notification.

Note: While it is technically feasible for the InterScan MSS server to relay notifications, we do not recommend it because notifications would not be sent if the server is incapacitated. See *Notification settings* starting on page 3-10 for more information.

---

5. In the **Email** field, type the email address to which notifications will be sent.
6. Type your company's name and mail domain name as it appears in the mail exchange (MX) record of your DNS server. If you want InterScan MSS to protect multiple domains, for example, dog.com, cat.com and fish.com, enter one of the domains into the setup program and proceed. When you have finished, go into the InterScan MSS console and:
   a. Update your DNS server's MX record so that Internet mail that previously went to dog.com, cat.com, and fish.com are now routed to InterScan MSS.
   b. Add the remaining domains to the **Allowed Relay Destinations** list under **Configuration** > **SMTP Routing** > **Receiver** > **Relay Control**.

c. Configure SMTP Routing settings for each domain. For more information, see *SMTP routing* starting on page 3-17.

Note: You cannot use the wildcard (*) in the installation program to select multiple sub-domains.

Selecting server locations for installation

1. The **Trend InterScan MSS Remote Installer** screen opens. Select the server(s) where you want to install InterScan MSS by browsing the domains in the left-hand pane. Double-click on the domains for a list of available servers. After you highlight the server name in this pane, click **Add**. The server name displays in the right target pane. Alternatively, type the server's name in the field under **Add server name** and repeat as necessary. Click **Next**.
2. In the **IMSS Setup--Server Logon** screen, enter a user credential with local (or domain) administrator privileges to the target server(s).

Note: You must be logged into the local machine with local or domain administrative privileges.

If you want the installation program to remember the logon credential for future installation/uninstallation sessions, click **Add** under the **Credential List**. If you have selected multiple target machines, the installation program prompts you for a new credential to log on to the target server. Click **Logon**.

3. The installation program attempts to log on to each computer that you have listed. Subsequently, the software is installed on all target machines simultaneously. The result of each attempt is shown in the **Analysis Status** column in the table.
4. Specify the folder where you want to install the software, and the folder name that will appear as a shortcut on your Windows **Start** menu. The default shortcut name is

What if installation fails on a target machine?

If a target machine's installation is unsuccessful, a message box displays with a summary when all of the installations conclude. Failed installations do not affect attempts on other target servers.

Trend Micro InterScan Messaging Security Suite. Click **Next** to start the installation.

Monitoring installation progress

1. View the progress of the installation under the **Installation Status** column of the **Remote Installer** window. Depending on your system resources and network connection speed, the installation may take several minutes.
2. The **InterScan Messaging Security System Monitor Service** loads on the target machine. Since this program is required by the InterScan MSS service, it cannot be manually closed; you can, however, minimize it. Shortcuts are only created on the target machine, not the machine performing the remote installation.
3. Click **Next** to display the installation status summary for all the target servers.
4. Click **Finish** to close the installation program.

Installation log files

Information about the installation process is logged in six log files. They are saved in a directory called \IMSS_RILOG under the root directory where Windows is installed (usually c:\IMSS_RILOG).

The log file names are:

- Isnt_Setup.txt
- isnt_{ServerName}_ISWI.txt
- RInstall.log.yyyy.mm.dd
- isnt_install.txt
- ccgi_install.txt
- CCGI_{ServerName}_ISWI.txt

Note: If you run the InterScan MSS installation program on a server that already hosts the program, backup copies of the .ini and .dat files are saved to the IMSS_RILOG directory on the system drive with the installation log files. If there is an error, you can use these backups to recover your old settings.

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

Both of these components require a Microsoft SQL database for data storage. This database can be either a SQL Server database or Microsoft's freely-distributable Microsoft SQL Desktop Engine (MSDE) database.

Note: The MSDE database software has a built-in limit of 2GB. If your database exceeds this limit, InterScan™ Messaging Security Suite will be unable to write new entries for the Network Reputation Service or SPS to the database. If you are in a high-traffic environment, or if you reach the 2GB limit, Trend Micro recommends using Microsoft SQL Server instead of MSDE.

The spam reporting and EUQ installation program provides an installer that will install MSDE if you do not already have a Microsoft SQL database installed.

Note: Only one instance of the spam reporting and EUQ component can be installed per database.

Configuring a data source name (DSN)

The InterScan MSS centralized spam reporting and Web-based EUQ components make database connections using a data source name (DSN) that identifies the database and the engine used to work with it. If the database is on a server other than the one where the components are installed, these tools require a DSN to connect to the database on that other server.

To configure the Data Source Name:

1. Click the **Start** button to display the **Start** menu.
2. Select **Settings > Control Panel**.
3. Select **Control Panel > Administrative Tools**.
4. Select **Administrative Tools > Data Sources (ODBC)** to display the **ODBC Data Source Administrator** dialog box.
5. Select the **System DSN** tab.
6. Click the **Add** button to display the **Create New Data Source** dialog box.
7. Select **SQL Server** from the list of drivers, then click **Finish**. The dialog box closes and the **Create a New Data Source to SQL Server** dialog box opens.
8. Type a **Name** for the data source, a **Description** (if desired), and select the name of the SQL Server to which you want to connect. Click **Next**.
9. The next screen prompts **How should SQL Server verify the authenticity of the login ID?** Select **With SQL Server authentication using a loginID and password entered by the user.**
10. In the **LogIn ID** and **Password** fields, type the login ID `sa` and the password that you set when you installed the database software.
11. Click **Next**. Windows checks the connection with the database, and the next page of the dialog box appears upon success.
12. Accept the default settings and click **Next**. In the next dialog box, also accept the default settings and click **Finish**.
13. A dialog box appears, summarizing the settings that have been made. Click **Test Data Source**.
14. The system attempts to connect to the data source with the listed settings. A Test Results message box appears with the message, “Test completed successfully!” Click **OK** to close this message box, then click **OK** again to close the setting summary dialog box.

15. The new data source appears in the list on the System DSN screen. Click **OK** to close the ODBC Data Source Administrator dialog box, then close the Administrative Tools window and the Control Panel window.

Installing the centralized spam reporting and EUQ software on your server

To install centralized spam reporting and EUQ:

1. Locate the IMSS package and open the `EUQPackage` sub-directory.
2. Run the `Setup.exe` program.
3. From the Welcome screen, click **Next**.
4. Read the license agreement, and if you agree to accept the license, click **Yes**.
5. Select an installation directory and click **Next**.
6. Choose a database type and location.
   a. To have the IMSS installation program install the MSDE database on this server and configure the database connection, select **Install MSDE** and type and confirm a **Password** for the MSDE "sa" user account.

      Note: This password will be used by both IMSS and the centralized spam reporting and EUQ tools to access the database.

   b. To use an existing database instance and preconfigured DSN:
      i. Select **Use existing**.
      ii. Click **Next**.
      iii. When prompted to **Choose Data Source**, provide the Data Source Name, then click **Next**.
      iv. Type the **Password** for this data source name and click **Next**.
      v. Select **Yes** when prompted to create an IMSS database on your server, then click **Next**.

7. Create an Administration Account for accessing the console.
   a. Type an account password.
   b. Confirm the password and click **Next**.
8. Note the ports that will be used to access the Administration console and End-user console and click **Next**.
9. Review settings and click **Next**.
10. Setup will install the necessary files and services to your computer.
11. Reboot:
    a. To allow Windows to start the centralized spam reporting and EUQ services, select **Yes, I want to restart my computer now**.
    b. To restart later, select **No, I will restart my computer Later**.

Updating the DNS server's MX record

Modify your DNS server's MX record so that Internet mail that used to be routed to your SMTP server is now routed to the machine hosting InterScan MSS.

Opening the IMSS management console

The InterScan MSS 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 locally, click **Start** > **Programs** > **Trend Micro InterScan Messaging Security Suite** > **Trend Micro InterScan Messaging Security Suite Web Configuration**.

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

```
http://<target server's IP address>/InterScanMssConfig.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. See *Viewing the management console using SSL* starting on page 2-28 for more information.

The default password for the InterScan MSS console is blank. To prevent unauthorized changes to your policies, we recommend that you configure a password as soon as possible. See *Management console password* on page 3-12 for more information.

Note: 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.

Opening the centralized spam reporting and EUQ console

The centralized spam reporting and EUQ console 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 locally, click **Start** > **Programs** > **Trend Micro InterScan Messaging Security Suite** > **Spam Admin Console**

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 will be the password you entered during installation. To prevent unauthorized changes to your policies, Trend Micro recommends changing the password regularly.

Note: 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 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 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

InterScan MSS's server can be used to 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 navigation panel, choose **Configuration** > **SMTP Routing** > **Receiver** > **Relay Control**. For more information, see *Relay control* starting on page 3-20.

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 message routing table and the domain shown in the message's destination address govern the delivery method used after messages are processed. 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) or a DNS server, depending upon the delivery method specified during installation. Messages destined to all other domains use a DNS server to resolve the destination address.

InterScan MSS queries the DNS servers listed in the **Configuration** > **SMTP Routing** > **Delivery** > **Domain-Based Delivery** settings. Initially after installation, this DNS server list is empty. If no DNS server names are entered into the message routing table, InterScan MSS uses the default DNS server from the InterScan MSS server's TCP/IP settings.

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

- In the navigation panel, choose **Configuration** > **SMTP Routing** > **Delivery** > **Domain-Based Delivery**.

For more information see *Domain-based delivery* starting on page 3-21.

Updating InterScan MSS

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

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

For more information about on-demand program updates, see *On-demand update (Update Now)* on page 3-14.

Configuring Scheduled Update

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

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

For more information, see *Scheduled update* starting on page 3-14.

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

Checking mail flow

To check the mail flow, send messages to the addresses in all of the domains that InterScan MSS has been configured to protect, and ensure that mail is successfully

delivered. Additionally, send messages to other domains to verify the delivery method (DNS or SmartHost) is configured correctly.

To view message processing status using the **System Monitor**:

1. In the navigation panel, choose **Configuration** > **System Monitor** > **System Status**.
2. Send test messages and watch the numbers increase in the **System Monitor** screen.

Viewing the management console using SSL

The InterScan MSS management console supports encrypted communication using SSL.

Here are some guidelines that you need to follow:

- Before attempting to install InterScan MSS, apply an SSL security certificate to the IIS server that will host InterScan MSS. If you have already installed InterScan MSS on an IIS server to which a SSL certificate has not been applied, uninstall the software, apply the certificate, and reinstall InterScan MSS.
- After installing InterScan MSS to an SSL-enabled IIS server, you have to modify a file that contains the management console's URL. Open the \TrendMicro\InterScan5\UI\intscan.url file and change the URL to the following:

  ```
  [InternetShortcut]
  URL=https://<server IP address>/InterScanMssConfig.html
  ```

Note: The intscan.url file must contain the actual IP address of the machine where InterScan MSS is installed. Using localhost or 127.0.0.1 will not display the Web console if accessed from an SSL-enabled IIS server. You can use the same URL to open the console from a remote machine.

- Make sure the version of SSL in your Web browser is compatible with the version used by your IIS server. For example, if you apply a 128-bit SSL certificate to your IIS server, make sure that your browser also supports 128-bit encryption.

Upgrading from the evaluation period

If you entered an evaluation Activation Code for InterScan MSS or Spam Prevention System (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 a valid Activation Codes in the Web console.

To enter Activation Codes:

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

Backing up and replicating data

This section describes the process of exporting settings from one InterScan MSS™ server and then importing them to another. This provides a shortcut to duplicating an existing InterScan MSS server's settings on a newly-rolled out server, without having to reconfigure using the Web-based user interface.

In addition, these processes are useful if you are using multiple InterScan MSS servers:

- In a clustered configuration to increase performance
- To backup data for later restoration (in case of emergency)
- To save a current policy configuration before making significant changes to settings

Migrating settings

You can import or export your settings from one InterScan MSS server to another.

Under *Exporting*, below, is a list of the files that should be backed up to save the virus scanning, relay control, delivery configuration, and the eManager™ rules/policies from an InterScan MSS server. These files can then be used to restore this configuration or migrate the settings to another InterScan MSS server, so that both machines have the same settings.

Exporting

To export (and backup) your settings from an InterScan MSS server:

1. On the InterScan MSS server that has the configuration that you want to export, make backup copies of the following files from the \Trend\IMSS directory (default installation path = c:\Program Files\Trend\IMSS):
   - conn_restrict.dat

     This file stores the InterScan MSS console settings under **Configuration** > **SMTP Routing** > **Receiver** > **Connection Control**.
   - localdomain.dat

     This file stores the domain settings from the **Allowed Relay Destinations** list under **Configuration** > **SMTP Routing** > **Receiver** > **Relay Control**.
   - rely_restrict.dat

     This file contains the **Permitted Senders of Relayed Mail** list under **SMTP Routing** > **Receiver** > **Relay Control**.
   - TmLogFlag.ini

     This file controls the debug logging level that is configured under **Configuration** > **Logs** > **Log Maintenance**.
   - IsntSmtp.ini

     This file is the main configuration file for InterScan MSS and contains a majority of the configuration settings from the Web console.
   - DomainTable.ini

     This file is the domain-based delivery table that stores the InterScan MSS console settings under **Configuration** > **SMTP Routing** > **Receiver** > **Connection Control**.

- POP3.ini

  This file stores information from the POP3 section of the Web console, such as settings and connections.

2. For policy backup, use the Windows Registry Editor (**Regedit**) to export the following registry entry:

   ```
   HKEY_Local_Machine\SOFTWARE\TrendMicro\ISNT5
   ```

Importing

To import (and restore) your settings on a new InterScan MSS server:

1. Install InterScan MSS on a second server. You must use the same program version and the exact installation path as the InterScan MSS server from which you exported the settings.
2. Open the Windows Registry Editor (**Regedit**) on the second InterScan MSS server and:

   a. As a precaution, backup the entire registry.

   b. Delete the ISNT5 registry tree.

   c. Import the registry information that was exported in Step 2 of the Exporting procedure.

Note: You can import registry data by choosing **Registry** > **Import Registry File...** from Regedit's main menu. Consult the Windows Registry Editor's Online Help for more information.

---

3. Copy the backup files listed under *Exporting* on page 2-30, into the \Trend\IMSS directory (default installation path = c:\Program Files\Trend\IMSS) of the new InterScan MSS machine. This step overwrites the existing files on the new server.
4. Proceed with one of the following:

   a. If the InterScan MSS machine from which you exported the settings is using an updated anti-spam database, or Outbreak Prevention Services (OPS) policy, copy the following files to the second InterScan MSS server:

   - \Trend\IMSS\ISNTSmtp\download\spam\TM_Trend$SE.xxx
   - \Trend\IMSS\ISNTSmtp\download\spam\TM_Antispam.xxx

- \Trend\IMSS\ISNTSmtp\download\opp\opp.xxx
- \Trend\IMSS\ISNTSmtp\download\MMP\massmail.lst

Note: The \download directory is created the first time you attempt to update your InterScan MSS server through the Internet. If you have not updated your program, the \download directory will not exist.

In the file path, "xxx" indicates the version number.

b. If the InterScan MSS server from which you exported the settings is not using the latest anti-spam, OPS files, or MMP files, copy the following files to the second InterScan MSS server:

- \Trend\IMSS\ISNTSmtp\TM_Trend$SE.xxx
- \Trend\IMSS\ISNTSmtp\TM_Antispam.xxx
- \Trend\IMSS\ISNTSmtp\massmail.lst

By default, InterScan MSS 5.0/5.01 does not include \Trend\Isntsmtp\opp.xxx.

Note: You must complete one of the above steps, because the registry data imported from the primary InterScan MSS machine contains some path information that relates to these files.

5. Reconfigure the receiver settings, where InterScan MSS binds to an IP address, by selecting **Configuration** > **SMTP Routing** > **Receiver** > **Settings**.

Note: In InterScan MSS 5.5, if you choose to bind to **All Interfaces**, you do not have to reconfigure the IP. But, as a precaution, you should confirm your IP settings.

6. After the settings are imported or migrated, monitor the second InterScan MSS server closely to ensure that it is working properly.

Removing InterScan MSS

InterScan MSS's installation program, setup.exe, can also uninstall the software. If you have customized the program's settings and want to preserve your customizations, you should save some .ini files and registry entries before uninstalling so that you can recreate your previous installation.

Saving your customized settings

If you are installing multiple instances of InterScan MSS for clustered servers, you can save your customized settings. These settings are stored in .ini, *.dat files, and registry entries.

To save your settings:

1. Save all .ini files under the root \Trend\InterScan MSS directory (conn_restrict.dat, DomainTable.ini, IsntSmtp.ini, rely_restrict.dat, localdomain.dat and TmLogFlag.ini) and under the \Trend\InterScan MSS\ISNTSmtp directory (TMeMgr.ini).
2. Export the registry entries under:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ISNT5
   ```

For more information about this process, see *Exporting* on page 2-30.

Restoring settings

If you reinstall InterScan MSS and want to restore your previous settings, do the following after the installation is complete:

1. Copy all the .ini and *.dat files listed above from your backup to the correct directory locations in the new installation.
2. Double-click on the *.reg file that contains all of your exported registry entries to import them to your new installation.

Note: To use your saved settings in a new installation of InterScan MSS, you must install the software to the same drive letter and path as your previous installation, because the configuration files contain absolute path information.

Using Setup to Remove InterScan MSS

Use the InterScan MSS setup program to remove the software. The program can be run from the server where you have installed the components or from a remote Windows NT or 2000 machine across the network.

Note: Do not attempt to uninstall InterScan MSS by running **Add/Remove Programs** from the Windows **Control Panel**. The InterScan MSS setup program installs several components, and the order of uninstallation is significant.

To uninstall InterScan MSS:

1. Run Setup.exe to start the installation wizard.
2. Click **Next**.
3. Click **Yes** to signify your agreement with the license and click **Next**.
4. Select **Uninstall InterScan Messaging Security Suite** and click **Next**.
5. After the InterScan MSS **Remote Installer** screen is displayed, select the server where InterScan MSS is installed and click **Add**.
6. Click **Next**.
7. Enter a credential with local administrator rights to log on to the target server and click **Logon**.
8. Click **Next** to start the removal process. Progress messages are shown in the **Remote Installer**'s window.
9. When the removal process finishes, click **Next**. Setup shows a summary. Click **Finish** to close the program.

Uninstallation log files

Setup writes log entries to a directory called \IMSS_RILOG under the root directory where Windows is installed (usually c:\IMSS_RILOG). These log entry files are:

- isnt_uninstall.txt
- ccgi_uninstall.txt

Chapter 3

Configuring InterScan™ MSS

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

The following topics are covered:

- Enabling notification using email or SNMP trap
- Changing InterScan MSS's message processing directories
- Changing the management console password
- Updating your virus pattern, scan engine, and spam database
- Viewing and maintaining log files
- Configuring the **SMTP Routing** settings
- Using the **System Monitor** for real-time status information
- Registering your software and updating an evaluation version to the full version

For more information about configuring antivirus protection, see *Using the Virus Filter* starting on page 5-1. Content filtering configuration is covered in *Filtering Content with the Spam Prevention Solution Filter (SPS)* starting on page 7-1 and *Filtering Content with the eManager™ Filtering Tools* starting on page 6-1.

Opening the InterScan MSS console

The InterScan MSS Web console can be viewed locally through a Web browser from the machine where the program was installed or remotely across the network.

Note: The default password for the InterScan MSS console is blank. To prevent unauthorized access, we recommend that you configure a password as soon as possible. See *Management console password* starting on page 3-12 for more information.

To view the console locally, click **Start** > **Programs** > **InterScan Messaging Security Suite** > **Trend Micro InterScan Messaging Security Suite Web configuration**.

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

`http://<target server's IP address>/InterScanMSSConfig.html.`

Using the target server's fully-qualified domain name (FQDN) rather than the IP address is also acceptable.

Note: If InterScan MSS is installed on a multi-homed machine that has multiple IP addresses, use the IP or FQDN of the **Default Web Server** in Internet Information Server.

As a security precaution, the InterScan MSS Web console times out after 20 minutes of inactivity and returns you to the password-entry screen.

Using online help

The InterScan MSS Web console includes online help that can be viewed 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, your questions have not been answered, see *Troubleshooting and Contact Information* starting on page 9-1 for additional information about accessing technical support, such as self-service support through Trend Micro's Web-based Knowledge Base.

Applying configuration changes

Configuration settings are saved in the system registry or an .ini file on the server. A copy of the registry/.ini file data is written into memory when the InterScan MSS 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 registry or.ini file and apply them. This resource-intensive task, if done frequently, would diminish system performance.

When you click **Apply Now**, InterScan MSS reads the new data from the registry/.ini file and applies the changes. Some configuration changes, such as changing the directories used for message processing or changing the mail settings, can only be changed by restarting the InterScan MSS service.

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

1. Settings applied automatically after saving

These configuration changes are applied automatically after they are set in the InterScan MSS console:

- Changes to the InterScan MSS console password. For more information, see *Management console password* starting on page 3-12
- Scan engine, virus pattern, and spam database **Update Now** settings. For more information, see *On-demand update (Update Now)* starting on page 3-14

- Proxy server settings. For more information, see *Configuring proxy settings* starting on page 3-13
- Scan engine, virus pattern, and spam database **Scheduled Update** settings. For more information, see *Scheduled update* starting on page 3-14

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

- All virus, eManager and **Program Log** viewing settings. For more information, see *Logs* starting on page 3-16
- Viewing and reprocessing messages in the **Retry Queue Viewer** (clicking **Deliver Now** automatically delivers the selected message in the queue; see *Viewing the Retry queue* starting on page 3-31)
- **Event Monitoring** settings. For more information, see *Event monitoring* starting on page 3-30

Note: When you make changes to the configurations listed above, which are applied automatically, the **Apply Now** button will be unavailable.

2. Settings immediately updated using Apply Now

Some configuration changes in the InterScan MSS console can be immediately enforced by clicking **Apply Now**. 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 scanning threads are suspended temporarily during the update process.

These configuration changes can be enforced immediately by clicking **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 3-10

Note: Notification settings are immediately applied to the InterScan MSS **System Monitor**.

- **Security** settings. For more information, see *Update* starting on page 3-13
- All **SMTP Routing** settings, except for the **Receiver > Settings > IP address** configuration where the InterScan MSS server is installed. These include:
  - **SMTP Routing > Connection** settings. For more information, see *Connections* starting on page 3-18
  - **SMTP Routing > Connection Control** settings. For more information, see *Connection control* starting on page 3-19
  - **SMTP Routing > Relay Control** settings. For more information, see *Relay control* starting on page 3-20
  - **SMTP Routing > Domain-based Delivery** settings. For more information, see *Domain-based delivery* starting on page 3-21
  - **SMTP Routing > Advanced Delivery** settings. For more information, see *Advanced delivery settings* starting on page 3-22
  - **SMTP Routing > Message** settings. For more information, see *InterScan MSS message settings* starting on page 3-23

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

- **System Monitor Exception Handling** settings. For more information, see *Exception handling* starting on page 3-9

Note: If you have made any configuration changes that have not yet been applied to the program, click **Apply Now** to dynamically apply your changes.

3. Settings applied after restarting the service

InterScan MSS does not apply some configuration changes until the service is restarted, including:

- Updating the **SMTP Routing Receiver** settings, including the InterScan MSS server's IP address, port and greeting message. For more information, see *Receiver settings* starting on page 3-17
- Modifying the processing, retry or postpone delivery queue directories. For more information, see *Mail processing queue directories* starting on page 3-11
- Changing any of the **Log Maintenance** settings, including the logging level, the log directory or the number of days to keep log entries. For more information, see *Log maintenance* starting on page 3-16

Note: After making these configuration changes, the **Apply Now** button is deactivated.

Security

InterScan MSS includes features to prevent it from being victimized by denial of service (DoS) attacks that result from receiving large (or multiple) messages and attachments. You can also configure how messages are processed in the event of program failure.

Security settings

InterScan MSS provides settings to control the types of messages and attachments it will accept for processing. Configuring the maximum layers of recursively-compressed archives, the maximum attachment and file size, and the maximum number of viruses that will be cleaned in a single attachment reduces the chance that InterScan MSS will be immobilized by a malicious DoS attack.

To configure InterScan MSS's security settings:

1. In the navigation panel, choose **Configuration** > **Security** > **Security Settings**.
2. Configure the maximum limits in the appropriate fields, overwriting the default values.
3. Click **Save** and then **Apply Now** to apply your changes to the current session.
4. Click **Apply Now** in the top-left corner of the screen

Compressed file scanning limits

Compressed files (zip, .lzh, etc.) can contain other compressed files. Since compressed files must be decompressed to be opened and scanned, scanning a recursively-compressed file with many layers is resource intensive. In addition, because the scanning engine can scan up to a maximum of 20 layers, recursively-compressed files can be used as a way to "smuggle" malicious code or inappropriate content past antivirus and content management software.

You can also set the maximum size of a file after decompression. This prevents malicious parties from launching a DoS attack against InterScan MSS using a "ZipOfDeath".

What is the "ZipOfDeath" vulnerability?

Some file types can be compressed with a high compression ratio, such as > 99%. A "ZipOfDeath" is a compressed file that expands greatly after decompression. For example, a 50 KB compressed file might expand to 3 GB. This can overwhelm your system resources and cause mail delays while the attachment is scanned. This vulnerability has been exploited to launch DoS attacks against SMTP-based antivirus and content management software.

Attachment and message virus scanning limits

If a message with a large attachment arrives at the InterScan MSS server, mail flow would be stopped while the scan engine checked for viruses. You can set the maximum amount of data (the total combined size of both the message and attachment) that will be processed.

A message with many file attachments could also be sent to intentionally disrupt the mail flow. If this happens, no additional messages can be processed until all of the attachments in the message have been scanned. Configure the maximum number of attachments per message to reduce your vulnerability.

What happens to the message if scanning is aborted?

If scanning is aborted due to exceeding a maximum value in the *Security Settings* screen, the filter action set for "Virus scanning aborted - message may contain viruses" will be performed. For more information, see *Choosing a filter action* starting on page 5-4.

Note: InterScan MSS counts both files and embedded objects within files towards the total number of attachments when determining if a message should be blocked. So a message that had a Word file with three embedded Excel spreadsheets would count as four file attachments.

Multiple virus-infected message limits

When InterScan MSS's scan engine detects a virus, it attempts to clean the file. Then it will rescan the file to confirm whether the cleaning attempt was successful. Regardless of whether the cleaning was successful, the engine continues to scan the file for additional viruses.

The message is not forwarded for final delivery until scanning is finished. An attachment that contains multiple viruses can disrupt the mail flow. Because an attachment infected with many viruses is most likely a deliberate attack against your network (there is no legitimate reason for a file to contain 100+ viruses), you can configure InterScan MSS to abort scanning after it detects of a set number of viruses. In addition, you can stop recording the virus infections to the log file to prevent multiple notifications about the same problem message.

eManager™ filter message size limit

Just as you can abort virus scanning of large attachments, you can configure the eManager filter to abort scanning large messages. This reduces your vulnerability to having large messages disrupt your mail processing.

Exception handling

If InterScan MSS cannot successfully process a message, you can choose an action to reduce the risk of a virus-infected or prohibited message being delivered.

The two types of exceptions are:

- InterScan MSS fails to process a message: This exception may occur when the system is out of memory or system handles, or may result from policy-setting errors. Anything that prevents InterScan MSS from processing a message is categorized as a processing failure.
- InterScan MSS receives an encrypted message: Encrypted messages cannot be scanned by the filter's antivirus scan engine or the eManager filter.

For more information on filter actions, see *Using filter actions* starting on page 4-7.

To choose an action for messages that cannot be processed:

1. In the navigation panel, choose **Configuration** > **Security** > **Exception Handling**.
2. Choose the filter action for each condition and click **Save**.

Note: Updated **Exception Handling** settings can be applied to your current InterScan MSS session by clicking **Apply Now** in the top-left corner of the screen. Otherwise the settings are loaded after restarting the program's SMTP scanning service.

General settings

The **General** portion of the **Configuration** menu provides settings that control notifications, queue directories, and the management console password.

Notification settings

You can be notified through email or SNMP trap when a virus is detected, a policy is updated, or the system requires attention.

1. In the navigation panel, choose **Configuration** > **General** > **Notification Settings**.
2. Configure the settings for all of the notification methods that you want to use—email or SNMP Trap.
   - In **Administrator email**, type the administrator's email address; remember to separate each entry with a semi-colon.
   - In **From address**, type the sender's email address.
   - If email notification messages contain non-English characters, enter the **Preferred charset**.
   - In **Message header**, type the header text.
   - In **Message footer**, type the footer text.
   - Entering "0" in any field is the same as not setting a limit.
   - Using SNMP trap notification requires a simple network management protocol (SNMP) server to receive the SNMP trap. Trap type is used to distinguish between different events.
3. Click **Save** when finished.
4. Click **Apply Now** in the top-left corner of the screen.

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.

Mail processing queue directories

The following default directories are used for the scan, postpone, and retry queues:

- Processing queue: ...\InterScan MSS\ISNTsmtp\mqueue
- Retry queue: ...\InterScan MSS\ISNTsmtp\bmqueue
- Postpone queue: ...\InterScan MSS\ISNTsmtp\postpone

During normal operation, most of the messages to be scanned and delivered are temporarily stored in the mqueue folder. If the connection to the downstream server is lost or there is a DNS look-up failure, messages are placed into the retry queue for later delivery.

What Happens to Messages in the Old Queue?

If you change the paths used by the processing, postpone and retry queues, messages that are contained in the old queue are not processed. Before defining the new queue, make a note of the old one(s) and then manually copy its contents to the new one(s) using your Windows Explorer. The program will start processing the messages when they are moved to the new queue.

To change the default paths:

1. In the navigation panel, choose **Configuration** > **General** > **Directories**.
2. Type the paths that you want to use for the **Processing**, **Retry**, and **Postpone Queues**.

   Note: Restart the InterScan MSS service to apply changes made to the **Directory** settings.

3. Click **Save** when finished.

   Note: The path must be a local directory path, for example d:\foldername. Due to performance and security considerations, UNC paths (for example, \\computer-name\shared-folder\) are not supported.

Management console password

Access to the InterScan MSS management console can be restricted by using a password to prevent unauthorized changes.

Note: The default password for the management console is blank after InterScan MSS is installed. If you forget your password, contact a Trend Micro technical support engineer for instructions on resetting it, or uninstall and then reinstall the software.

To configure or change the management console password:

1. In the navigation panel, choose **Configuration** > **General** > **Password**.
2. Enter the existing password then enter and confirm your new password. The new password will take effect immediately after you click **Save**.

Services

The Services section of the management console provides tools to configure and activate or deactivate InterScan MSS services.

Settings

In the **Settings** 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 type of mail handling you want, in the navigation panel, choose **Configuration** > **Services** > **Settings**. Select SMTP or POP3 mail handling and click **Save**.

Enabling or disabling an adaptor

This section discusses the differences between disabling SMTP and POP3 adaptors.

Note: You must restart the InterScan MSS service to enable/disable the SMTP and POP3 adaptors.

SMTP

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

POP3

If you disable the POP3 adaptor, InterScan MSS will not act as a proxy for POP3 mail. If you enable the POP3 adaptor but disable scanning, InterScan MSS will still act as a proxy for POP3 mail, but will not scan it. To disable scanning, choose **Configuration** > **POP3** > **Settings**, and clear **Enable POP3 Scanning**.

For more on POP3 scanning, see *POP3 mail scanning* starting on page 3-23.

Update

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

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 suspicious virus-like behavior and cleans viruses when they are detected. The SPS rules used by Spam Prevention Solution are also updated periodically.

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 3-15 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.

1. In the navigation panel, choose **Configuration** > **Update** > **Proxy Settings**.
2. Select **Use a proxy server** and enter the proxy server's name, port, and authentication information.
3. Click **Save**. The new proxy settings are immediately applied 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.

On-demand update (Update Now)

To update the virus pattern and spam database:

1. In the navigation panel, choose **Configuration** > **Update** > **Update Now**.
2. Select the components that you want to update. Newer components, if present, are denoted with a red **Update Now!** message.
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**.

Scheduled update

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, choose **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: The new **Scheduled Update** settings are immediately applied to the **InterScan MSS Scheduler** after clicking **Save**.

Rolling back an update

After updating to a new virus pattern file, InterScan MSS keeps the old pattern files on the server.

Note: The virus filter always uses the pattern file with the largest three-digit 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 the file \Trend\InterScan MSS\ISNTSmtp\lpt$vpn.###, where ### is three digits representing the pattern file version.
4. Verify that there is another virus pattern file in the \Trend\InterScan MSS\ISNTSmtp\ path where the pattern version is less than the one you deleted.
5. Restart the InterScan MSS service.

Logs

Logs retain important information about security and program events for InterScan MSS.

Viewing logs

1. In the navigation panel, choose **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 program's logging behavior, 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, choose **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, which policy is matched, which filter has been executed, and which outcome has been 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 was 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 logs to be retained.
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, the oldest log files are deleted.
6. Click **Save**.
7. Restart the InterScan MSS service to apply your new log settings.

SMTP routing

Before InterScan MSS can start scanning messages to and from your network, configure its built-in SMTP server.

Receiver settings

InterScan MSS includes its own SMTP server with fully configurable IP address, SMTP greeting, and connection time-out settings. In addition, you can control the servers from which InterScan MSS will receive messages, and which servers are allowed to relay messages through it.

Server identity (settings)

Specify the IP address and port to which InterScan MSS will bind, and the greeting message received by other SMTP servers after connection.

To configure the InterScan MSS IP address and SMTP greeting:

1. In the navigation panel, choose **Configuration** > **SMTP Routing** > **Receiver** > **Settings**.
2. Use the **IP address** (or preferably the FQDN) pull-down menu to select the IP address of the server where InterScan MSS has been installed.

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 the **Port** field, type the port number. In the **SMTP server's greeting message** field, type the greeting text.
4. Click **Save**.
5. Click **Apply Now** in the top-left corner of the screen.

Connections

InterScan MSS's built-in SMTP server accepts messages from other SMTP servers and, after processing is complete, passes these messages on. You can configure how these connections are handled.

To configure InterScan MSS's connection settings:

1. In the navigation panel, choose **Configuration** > **SMTP Routing** > **Receiver** > **Connections**.
2. In the **Connections** screen, you can configure:
   - The SMTP server disconnection timeout period
   - The maximum number of simultaneous connections
   - Whether to perform a reverse DNS lookup on incoming messages

What is Reverse-Lookup?

Reverse-lookup confirms the identity of the connecting host. When InterScan MSS receives a TCP connection request, it can get the source IP address of the remote computer. After a TCP connection is established, the remote computer sends a "HELO(EHLO) domain-name" SMTP command to InterScan MSS, which uses the "domain-name" to query DNS server(s) and the IP address of that domain. If the IP address matches the remote computer's IP address, the reverse-lookup was successful.

Note: Performing a reverse lookup on received messages prevents connection spoofing. However, enabling reverse-lookup may degrade InterScan MSS's performance.

3. Click **Save**.

4. Click **Apply Now** in the top-left corner of the screen.

Connection control

For added control, you can limit which SMTP hosts are allowed to connect to the InterScan™ Messaging Security Suite server. This process is performed by adding IP addresses or IP address ranges to a list which you can 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 the host is an open relay being used by spam senders.

To control which SMTP hosts are allowed 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, choose **Configuration** > **SMTP Routing** > **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 are allowed to relay messages through your InterScan MSS server.

Unscrupulous people who attempt to relay messages through an SMTP server are a common challenge for mail administrators. Spam senders 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 4-25.

InterScan MSS manages relay control by:

- Restricting relay to specific local domains: All hosts are allowed 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 IP or IP range: Only hosts that you specify (**Permitted Senders of Relayed Mail**) are allowed to relay messages to hosts not in the **Allowed Relay Destinations** list.

Essentially, 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: A blank **Permitted Senders of Relayed Mail** list means no servers can relay messages to the Internet using InterScan MSS.

To set relay privileges:

1. In the navigation panel, choose **Configuration** > **SMTP Routing** > **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**.
5. Click **Apply Now** in the top-left corner of the screen.

Delivery settings

InterScan MSS is a gateway product. that hands off mail to another SMTP server or MTA that can resolve the final destination. You can configure whether this process, based on the recipient's domain name, is performed using **DNS** or **SmartHost**.

Domain-based delivery

InterScan MSS routes email based on the recipient's domain. You can specify the routing method for **DNS** or forwarding to **SmartHost**. When you have multiple **SmartHosts** or **DNS** servers on the list, InterScan MSS performs load balancing.

1. In the navigation panel, choose **Configuration** > **SMTP Routing** > **Delivery** > **Domain-Based Delivery**.
2. The **Domain-Based Delivery** screen shows how mail destined for a specific domain is currently configured to be processed. To view or change a given domain's delivery method, click **View** in the **Details** column.

To create a new delivery method:

1. In the **Domain-Based Delivery** screen, click **Add**.
2. Enter the destination domain and then:
   a. Configure the DNS server(s) that should be used to resolve the destination domain, or
   b. Specify **SmartHost** to perform delivery.

   The order that server names appear in the DNS or SMTP server list dictates priority.
3. Click **Apply Now** in the top-left corner of the screen.

Advanced delivery settings

InterScan MSS includes optional delivery settings that you can use to customize how the SMTP server processes messages.

To customize your SMTP delivery settings:

1. In the navigation panel, choose **Configuration** > **SMTP Routing** > **Delivery** > **Advanced**.
2. Configure the following parameters:
   - **Deferrals**: If a message cannot be delivered on the first attempt, the retry interval and the duration specify the frequency and length of time before InterScan MSS will attempt to re-deliver.
   - **Advanced**: When a message cannot be delivered on the first attempt, it may "hop" around a route of servers on the Internet. You can configure the maximum number of hops a message can take before delivery attempts are aborted. In addition, you can configure a masquerade domain that overwrites the host portion of an email address.
   - "**Received" Header Settings**: To prevent others from knowing that a message was received by InterScan MSS's server, select **Do not insert SMTP "Received" header when processing messages**.
3. When finished, click **Save**.
4. Click **Apply Now** in the top-left corner of the screen.

"Hops" and masquerade domains

Configuring the "hop" count prevents messages from indefinitely "looping", i.e., mail server A routes a message to mail server B. In turn mail server B routes the message to mail server A, etc.
A masquerade domain replaces the local domain name listing in the "Mail From" lines in the SMTP protocol. This prevents others from seeing the identity of your internal SMTP servers.

InterScan MSS message settings

To prevent message delays, you can enforce the maximum message size, the maximum data size per session, the maximum number of messages per connection, and the maximum number of recipients per message. Messages will not be received if they exceed the maximum limits that you configure.

To set message limits:

1. In the navigation panel, choose **Configuration** > **SMTP Routing** > **Message**.
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**.
4. 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. The sending SMTP server is then expected to retransmit the remaining recipients in another session.

POP3 mail scanning

In addition to SMTP traffic, InterScan MSS can scan POP3 messages at the gateway as they are retrieved by clients in your network. Even if your company does not use POP3 email, your employees might want to access their personal POP3 email accounts using mail clients on their computers, which creates points of vulnerability on your network when left unscanned.

How It Works

The InterScan MSS POP3 scanner acts as a proxy, positioned between mail clients and POP3 servers, to scan messages as they are retrieved.

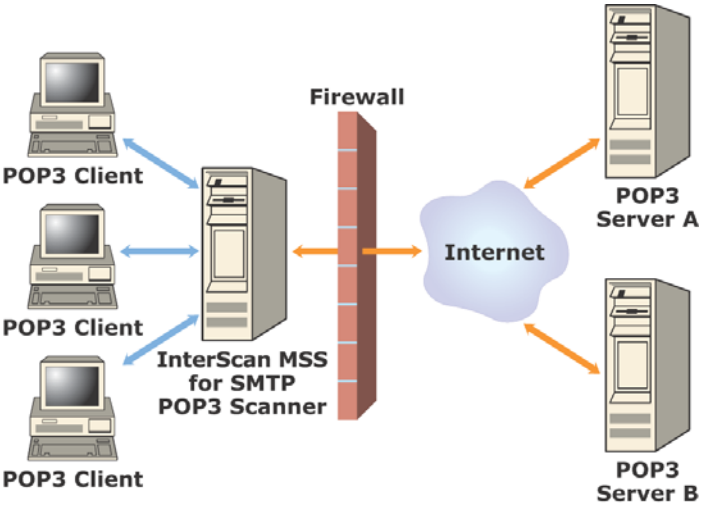


FIGURE 3-1. How POP3 scanning works

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. These connections should be used 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 the POP3 data flow is scanned.

In addition, configuration changes must be made to mail clients requiring them to retrieve messages only through the InterScan MSS server. A utility called the **POP3 Client Tool** is provided to assist with making configuration changes on the Eudora 5.2, Microsoft® Outlook® and Outlook Express® 6.0 mail clients. The **POP3 Client Tool** is packaged as an ActiveX® control so that users can run it from a Web page.

Note: The **POP3 Client Tool** only works under Internet Explorer on the Windows platform.

If your network's users need to connect to a POP3 server that requires an APOP or NTLM authentication, or you need to manually configure a mail client that is not supported by the **POP3 Client Tool** ActiveX control, see *Manually configuring email clients* starting on page 3-28.

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, choose **Configuration** > **POP3 Scanning** > **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.
4. Set the number of **Simultaneous User Connections**. This parameter controls the number of clients who can retrieve their POP3 messages at the same time, which impacts performance. The default value is 5, which is the recommended value. If you have installed InterScan MSS on a server with multiple CPUs, you can adjust this number to take advantage of the increased processing power.

5. If a POP3 message triggers a filter that causes the message not to be delivered, a message containing the **Status Message Text** is delivered instead. The action performed on the undelivered message depends on the policy actions associated with the filter, such as **delete**, **forward**, or **quarantine**.
6. Click **Save**.
7. Click **Apply Now** in the top-left corner of the screen.

Users must run the **POP3 Client Tool** or manually update their configuration to reconfigure their mail clients to retrieve email through the InterScan MSS POP3 proxy with the updated settings. For more information on using the POP3 Client Tool to configure mail clients, see *The POP3 client tool* on page 3-27.

Connections

You can specify the ports on the InterScan MSS server that will be used 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, choose **Configuration** > **POP3** > **Connection**.
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, choose **Configuration** > **POP3** > **Connections**.
2. Click **Add**.
3. Under **Inbound POP3 Port**, the port on the InterScan MSS server that will accept POP3 traffic for that connection is shown. Type the port that you want to use.
4. Under **POP3 Server**, the properties of the POP3 server are shown. 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. Clicking **Save** also updates the **POP3 Client Tool**'s POP3.ini file with these POP3 server settings.
6. Click **Apply Now** in the top-left corner of the screen.

Once you have created or modified a generic connection, users must run the **POP3 Client Tool** or manually adjust their configuration to reconfigure their mail clients to retrieve email through the InterScan MSS POP3 proxy with the updated settings. For more information, see *The POP3 client tool* on page 3-27.

To delete a POP3 connection:

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

The POP3 client tool

The **POP3 Client Tool** does the following:

- Configures any available POP accounts when executed.
- Only configures the generic connection defined in the InterScan MSS console connection settings. (You can define only one generic connection type.)
- Replaces the client's POP server address with the InterScan MSS proxy IP address.
- Appends the client's pre-existing POP server address after the account name, separated by a "#" delimiter.

This tool modifies Eudora 5.2, Outlook and Outlook Express 6.0 email clients to enable POP3 mail access through the InterScan MSS POP3 proxy. For detailed information on manually configuring email clients, see *Manually configuring email clients* starting on page 3-28.

Note: The **POP3 Client Tool** uses settings that you enter on the POP3 scanning **Settings** screen of the InterScan MSS management console. If the POP3 scanning **Settings** are changed, you must run the **POP3 Client Tool** to reconfigure mail clients with the new settings or users must adjust their client settings manually.

Running the POP3 client tool from a web page

To allow your users to reconfigure their email clients automatically using the **POP3 Client Tool** they can visit:

```
<InterScanMSS machine name>/InterScanPOP3ClientTool.html
```

This URL is where you will be prompted to run an ActiveX control.

Manually configuring email clients

In addition to using the **POP3 Client Tool** to automatically reconfigure mail clients, users can also manually configure their POP connection settings. Manual configuration is useful mainly when the client requires a specific, dedicated connection to their POP3 server through the InterScan MSS proxy.

Generic

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

In addition, 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**.

Dedicated

If the POP3 server requires authentication, you can still use the **POP3 Client Tool**. This step, however, requires a dedicated connection to be specified in InterScan MSS to handle the proxy request.

The primary benefit of defining a dedicated connection is that InterScan MSS can specify the location of the original POP server, which allows the user name to be preserved without modification.

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 dedicated connected settings of InterScan MSS.

System monitor

Keeping track of the InterScan MSS server's status helps identify potential problems before they affect the message flow.

System Status

The **System Status** screen provides real-time system performance data. You can check the volume of messages in the processing and retry queues, the number of messages processed since the service was started (including undeliverable messages), and the number of viruses detected.

To view the system status:

1. In the navigation panel, choose **Configuration** > **System Monitor** > **System Status**.
2. Click **Refresh** to update the view.

Event monitoring

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

The administrator is notified if:

- There are more than the configured number of messages in the delivery queue
- A scheduled update is attempted (successful or unsuccessful)
- Scanning service stops for more than the configured amount of time
- Disk space in the processing queue folder falls below the configured amount

Excessive messages in the delivery queue
A large or growing delivery queue is a symptom of messages not being delivered. Check your network and SMTP Routing Delivery settings. Also check the **Retry queue** to find out what is happening.

To configure events for which you want to be notified:

1. In the navigation panel, choose **Configuration** > **System Monitor** > **Event Monitoring**.

2. Select the fault conditions about which you want to be notified 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.
5. Click **Save**.

You must configure the notification settings for the method(s) that you choose to use. For more information, see *Notification settings* on page 3-10.

Note: Updated **Event Monitoring** settings are applied to the InterScan MSS System Monitor immediately after you click **Save**.

Viewing the Retry queue

If a message cannot be delivered on the first attempt, it is moved to the **Retry queue**, pending another delivery attempt. You can view the messages that are in the **Retry queue** and view the first 1KB of data in the message. If a message cannot be delivered within the configured retry interval and period, InterScan MSS deletes the message and sends a non-delivery receipt (NDR) to the sender. See *Advanced delivery settings* starting on page 3-22 for more information about configuring the retry interval and period.

If needed, you can immediately force-deliver messages in the delivery queue without waiting for the retry interval to elapse.

To manage your delivery queue:

1. In the navigation panel, choose **Configuration** > **System Monitor** > **Retry Queue Viewer**.
2. Messages that are currently in the **Retry** queue are displayed in the **Retry Queue Viewer** screen.
3. Select the message(s) for which you want to immediately retry a delivery attempt and click **Deliver Now**. For more information about a message, click the **view** link next to the message.

Undeliverable messages (Badmail folder)

By default, messages that remain undeliverable after the maximum retry interval and period will be deleted. However, you can optionally move undeliverable messages to the “badmail” directory by modifying the IsntSmtp.ini file located in the \Trend\InterScan MSS directory.

Note: The badmail directory is \Trend\InterScan MSS\isntsmtp\badmail. It cannot be modified.

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
- Testing your policies

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.

  The **Antivirus Filter** has several filter results, and each can perform a different filter action. Content management filters have two possible results—the message content either triggers or does not trigger the filter.

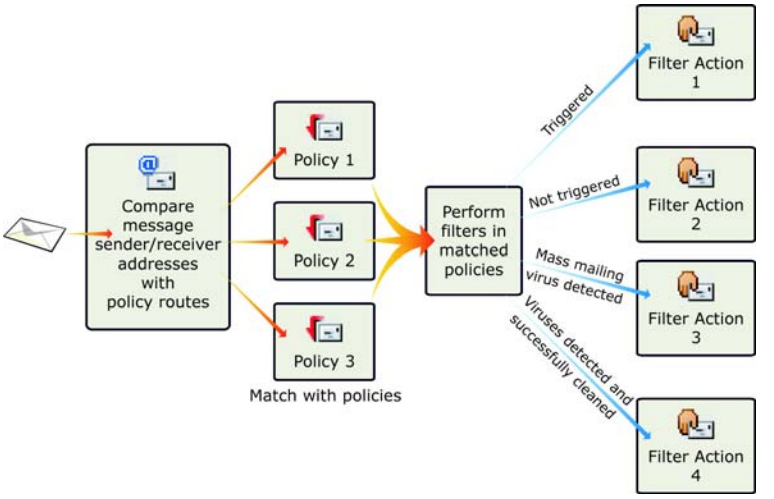


FIGURE 4-1. Simplified Policy Manager process flow

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 for SMTP filter.

If you have activated SPS you also have access to spam 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, choose **Policy Manager** > **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, choose **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, choose **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 remove 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, choose **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, choose **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 InterScan MSS's policies perform tests on messages and their attachments.

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

- Mass mailing virus detected
- Virus(es) detected and successfully cleaned
- Virus scanning aborted—message may contain viruses
- Virus(es) detected but some/all were not cleaned
- No virus detected

For filters using the eManager for SMTP 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 five 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 that was entered during installation. For more information about changing this address, see *Notification settings* starting on Page -10.

- **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 spam 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, viruses cleaned 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 for SMTP 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, choose **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 **Move**, **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 3-10.

- 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, choose **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, choose **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 SPS 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, choose **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 newly-created quarantine area.

Changing a quarantine area

To change the location of a quarantine area:

1. In the navigation panel, choose **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, choose **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 some of them were quarantined by a content filter that was too strict and was triggered by innocent messages. You can reprocess the messages after you have changed the content filter's properties
   - **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, choose **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, choose **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.

Viewing quarantined messages

You can view messages in quarantine areas using the quarantine viewer. This view provides detailed information about the message, including the sender, recipient, the time the message was sent, and the name of the file in the quarantine area that contains this message.

> **Note:** The quarantine viewer presents the first 128KB of text (under Linux) or the first 64KB of text (under Unix) from the message body in an unformatted form.

To view quarantined items:

1. Click **Policy Manager > Quarantine Area**.
2. Select a quarantine area and click **View**.
3. The next screen displays a list of quarantined messages.
4. To see the details of a quarantined message, click **View** in the **Details** column.

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**, **Virus**, which scans all messages and message attachments using the virus pattern file.

In addition, it contains the following disabled content management filters:

- **Spam Signature**: Compares message content with a database of expressions commonly found in spam email messages
- **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
- **SPS Filter**: This filter is available only if you have activated SPS. The SPS filter is based on sophisticated content processing and statistical analysis technology.

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 the **Spam Signature Filter**, you can change which parts of the message are compared to the spam signature database—the header, or the header and the body. See *Filtering messages using the spam signature filter* starting on page 6-4.
- 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 Filter** settings, see *Fine-tuning the SPS Filter* on page 7-10.

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 for SMTP 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.

SPS filter settings

The filter status and availability settings for the SPS 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.

SPS Filter Status

For SPS 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 SPS 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 Virus Filter* starting on page 5-1.

eManager™ filters

The following filters use the eManager for SMTP 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 SPS filter, the filter is shown during the evaluation period. If you do not upgrade to the full version, all SPS 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 6-11.
- 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 6-15.
- 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 6-3.
- The **Spam Signature Filter** detects spam by comparing messages with Trend Micro's spam database. For more information, see *Filtering messages using the spam signature filter* starting on page 6-4.

SPS filter

For complete information on using the SPS 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, choose **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**. This route is configured under the isntsmtp.ini's [IsntPOP3Adapter.dll] section:

- POP3From=
- POP3To=

By default, the .ini file already contains:

- POP3From=POP3FromLabel
- POP3To=POP3ToLabel

To define the route information, with the default .ini setting, enter *POP3FromLabel@** in the **From** field and *POP3ToLabel@** in the **To** field.

Note: The domain must be the wildcard "*" for the **To** and **From** fields.

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 *POP3 mail scanning* starting on page 3-23.

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 4-20.

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:

- Mass mailing virus detected
- Virus(es) detected and successfully cleaned
- Virus scanning aborted—message may contain viruses
- Virus(es) detected but some/all were not cleaned
- No virus detected

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

- Triggered (matches filter settings)
- 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 Virus Filter

This chapter explains how to use the **Virus 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 **Virus Filter** in the **Global Policy**:

1. In the navigation panel, choose **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

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, choose **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:

- Mass mailing virus detected
- Virus(es) detected but some/all were not cleaned
- 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 encrypted messages cannot be opened, they cannot be analyzed by the scan engine. Encrypted messages are processed based on your exception handling configuration. For more information, see *General settings* starting on page 3-10.

Examples

To help understand how the filter actions work, here is an example:

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. Viruses are categorized by malicious code, replication, and payload types. When the **Virus 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 for SMTP 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. In addition, eManager provides a spam signature filter that provides a high level of spam detection with a low risk of false-positives.

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 6-11).
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.

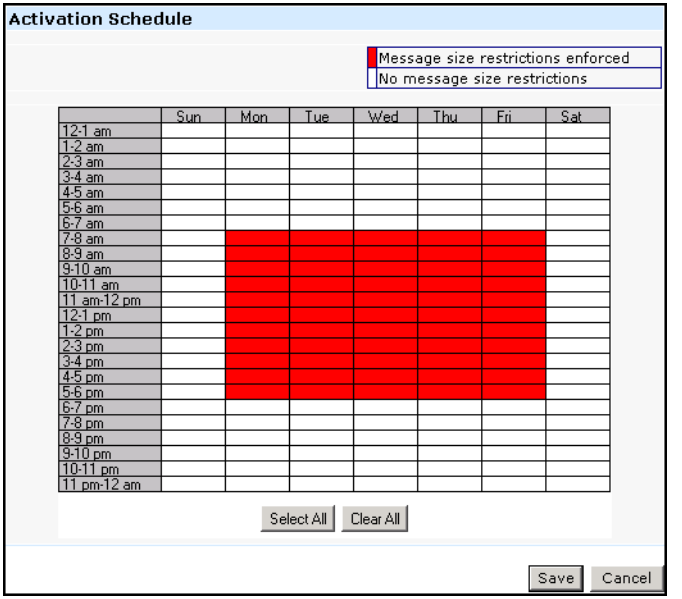


FIGURE 6-1. Message size filter—activation schedule

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 for SMTP 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 for SMTP filter's built-in operators, see *Using complex expression syntax* starting on page 6-18.
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 using the spam signature filter

When using the **Spam Signature Filter**, choose the message sections that you want to scan:

- **Enabled for message subject:** This option checks the message headers using TM_Trend$SE. The processing rate is faster than checking the mail body.

- **Enabled for both message subject and body:** This option results in a higher detection rate, at the expense of the mail processing rate.

Understanding spam signature filtering

The **Spam Signature Filter** detects spam messages by comparing message content with spam databases. You can automatically update the spam databases by choosing, in the navigation panel, **Configuration** > **Update > Scheduled Update**.

The file names for the spam databases are:

- TM_Trend$SE.### (### is the database version) contains message header characteristics, (subject, **From** and **To** fields, of known spam messages).
- TM_AntiSpam.### contains typical keyword expressions that have appeared in spam messages. Keywords can be a phone number, a URL, or other keyword expressions such as “Get rich in 30 days”.

How is the spam signature database developed?

Trend Micro’s team of spam collectors add identifying characteristics of spam email to the databases. Since spam senders frequently change their email addresses, identifying characteristics like Web sites or telephone numbers are used to detect them. If you receive a suspected spam message that our filter fails to detect, forward it (including all mail headers) to *spam@trendmicro.com*. We may add it to the database.

To verify the version of the spam database currently in use, in the navigation panel, choose **Configuration** > **Update** > **Update Now**.

Working with the spam signature filter

To create or modify the **Spam Signature Filter**:

1. Select one of the following options:
   - **Enabled for message subject.**
   - **Enabled for both message subject and body.**
2. Click **Next**.
3. Verify your filter parameters and click **Next**.
4. Using the pull-down menus, select filter actions and click **Save**.
5. You are returned to the policy screen where you can see your newly-created filter in the list.

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**, **Block HTML Script Messages** are types of **Advanced Content Filters**.

To see an example of this filter, in the navigation panel, choose **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 6-10.

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 Complex Keyword Expression Syntax on page 6-11.
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 6-25.

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 for SMTP 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 6-26).

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 6-13.
   - **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**.
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.

Will changing the attachment's file extension avoid attachment blocking?

No. The eManager for SMTP filter does not rely on a file's extension to determine the file type, but instead performs an internal analysis of the file.

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 for SMTP 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 for SMTP 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 newline 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**
[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 for SMTP filter uses several characters to parse the keyword expression into tokens. Words between these characters (known as separators), become a token.

The spam signature filter 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 for SMTP 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
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:

   [drive]\Program files\Trend\IMSS\ISNTSmtp
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 from Windows 2000/NT Service Manager.

   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 for SMTP 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 6-20.

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 (i.e, 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 filter**, 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 **Filter Type**, click **Edit**.
2. From the **SPS 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 filter:

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. Choose whether the text string scanning should consider case, and click **Next**.
6. Enter the string(s) to match.
7. 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

Working with the Centralized Spam Reporting and Web-based 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 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

Working with the Web Quarantine 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 too 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 Microsoft SQL database to index spam messages for end user retrieval. The freely-redistributable Microsoft SQL Desktop Environment (MSDE) is included in the installation package. You may also use Microsoft SQL Server 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 Web Quarantine Component

To use the Web quarantine tool, you must have installed a database and the Web quarantine component. This component provides a Web server, 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 Spam console to listen on port 8447 for the administration console.
- The installation program configures the Web quarantine to listen on port 8446 for end user traffic.

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 be access this server using their Web browser.

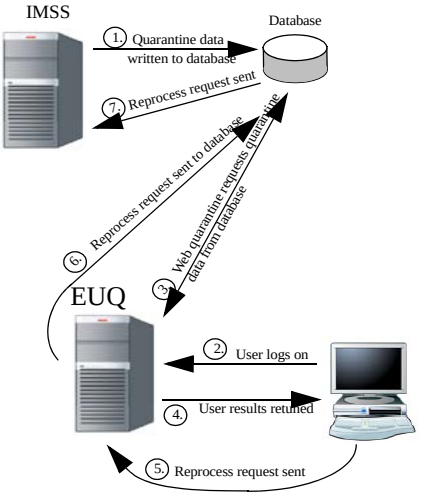


Figure 8-A: Web quarantine topology where components are on different servers

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.

For more information on installation topologies, see *Special information about Web End-user Quarantine (EUQ) and Network Reputation Service (NRS)* starting on page 2-7.

Enabling Web 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.

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. Configure LDAP connection settings by clicking **Web Spam Quarantine** > **LDAP Settings** in the left navigation panel.
3. 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.
4. Open the End-User Access screen in Web console by clicking **Web Spam Quarantine** > **End-User Access** in the left navigation panel.
5. Select the **Enable access** check box.

6. Set the **Approved Senders Setting** for each Web quarantine user.

   Note: The number of approved senders that are stored in the database will have an affect on system performance and message throughput. The more Web quarantine approved sender entries that exist, the longer the database query to look up the entries will take.

7. Select users and groups from the **Select LDAP groups to enable access** field.
8. Type a group or user name and click **Search** to find users or groups.
9. Click **Add** to move user and groups to **Selected Groups**.
10. Click **Save**.

Understanding Message Handling

- When IMSS receives a message with multiple recipient, it 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 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 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 20 days, spam messages will be stored in the spam quarantine, and accessible to the end user, for 20 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 with an "Unlimited" expiration are deleted from the database after 15 days.

Web-Quarantine and the Database

When a message is processed by InterScan Messaging Security Suite and quarantined by an SPS filter, it is placed in the quarantine directory on the server where it is processed. Periodically, the Web-based quarantine agent on the IMSS server checks the spam quarantines for new messages and indexes them in the database. Because this is a periodic task which occurs every three minutes, messages placed in the quarantine area by the SPS filter are not available to end users immediately after processing.

Understanding Approved Sender Lists

The Web-based quarantine tool allows users to add entries to the approved senders list, which allows these messages to be delivered even if they are flagged as spam by the SPS filter. However, the Web-based quarantine approved sender list and the IMSS SPS filter approved sender lists are independent. The InterScan Messaging Security Suite approved sender list applies to all SPS filters; the Web-based quarantine approved sender list does not. If a user adds a sender to their list, it will not be added to the IMSS SPS filter approved sender list automatically.

The InterScan Messaging Security Suite approved senders list for SPS uses a real-time mechanism. This means that when the administrator adds an entry to the approved sender list it takes effect immediately. The Web-based quarantine approved

sender mechanism is not real-time. It is applied by the IMSS Web-based quarantine agent on the IMSS servers. If a user adds approved senders to their individual list, new coming messages that are flagged as spam by SPS still will be quarantined first. Quarantined e-mails are processed by the Web-based quarantine agent. Messages sent from senders that are in an individual user's approved senders list will be released from the quarantine. Therefore, there may be a short delay after clients set their approved senders list before messages are delivered.

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.

For example, a user that logs on to their Windows 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.

The Web-based quarantine tool uses the LDAP `userPrincipalName` to look up the `mail` attribute for that account. Messages sent to the address specified in the `mail` attribute are available to the user.

Note: 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.

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, neither *dan@example.com* nor *jennifer@example.com* will see it.

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 an 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

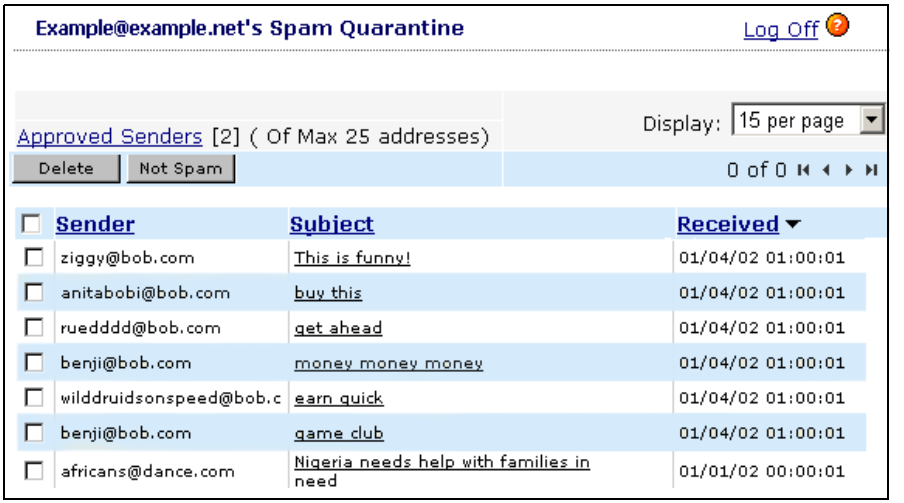
Your administrator should provide you with a URL that will allow you to access the Web quarantine console. Open your browser and type that address into the **Address** field to open the console. You may also want to add the address to your bookmarks to make accessing the tool easier in the future.

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

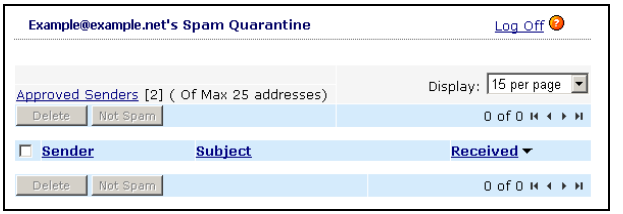
When the console opens, you will see the main page, which provides a list of messages that were sent to you that are in the quarantine. From here, you can delete them or tag them as Not Spam.



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.

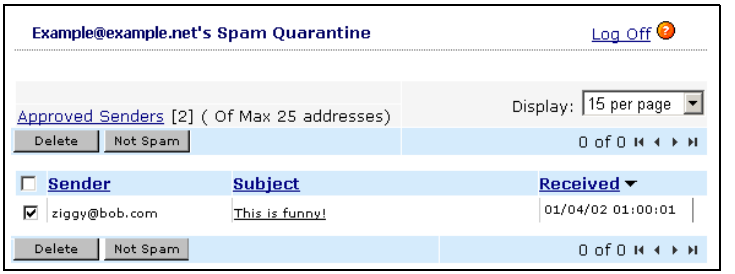
3. From here, you can choose to delete the message or add the sender to the Not Spam list.
4. To close the message viewer, click **Back to List**.

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.

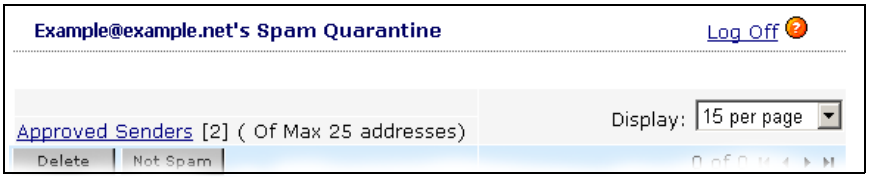
Note: You can select multiple messages by selecting them in the same way. To select all the messages that are currently being displayed, click the checkbox at the top of the column.

Managing Approved Senders

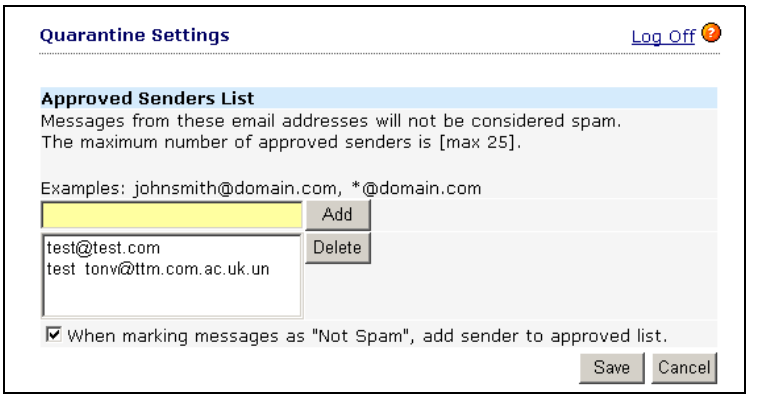
InterScan MSS allows each user to add sender addresses and domains to an individual Approved Senders List that prevents messages from these senders from being identified as spam. For example, if you add *joe@example.com* to your approved senders list, future messages from *joe@example.com* will not be 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.

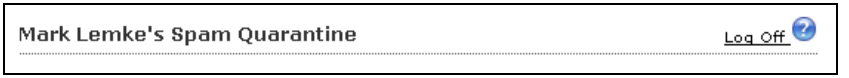
2. Click **Save**.

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

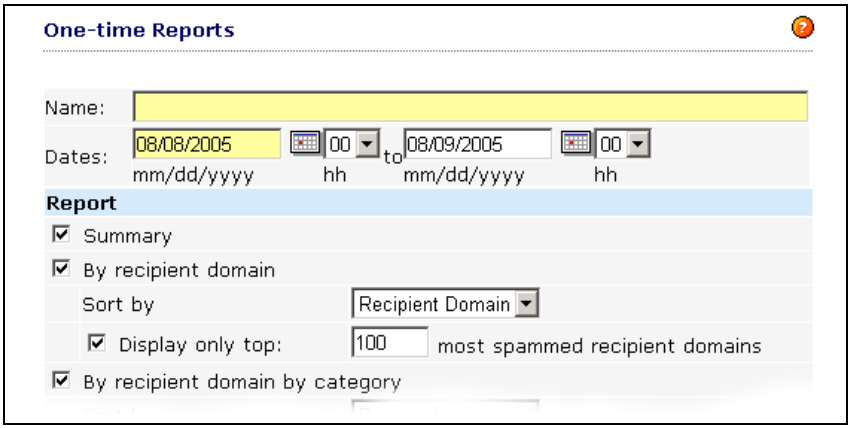
The reporting capabilities of InterScan Messaging Security Suite allow you to monitor messaging traffic and the effect of spam policies. You can generate these reports on a preset schedule, or as needed. You can configure them to provide an overall summary, or detailed information. IMSS generates reports as HTML files, which 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 **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.

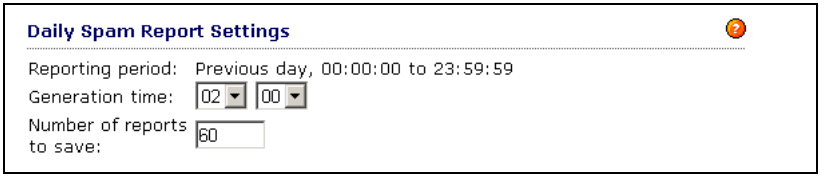
Some InterScan MSS reports are run on a schedule. You can configure them for generation on a daily, weekly, or monthly basis. Trend Micro strongly recommends configuring report generation for non-peak messaging traffic times as generating exhaustive reports that require numerous calls to the IMSS database (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:

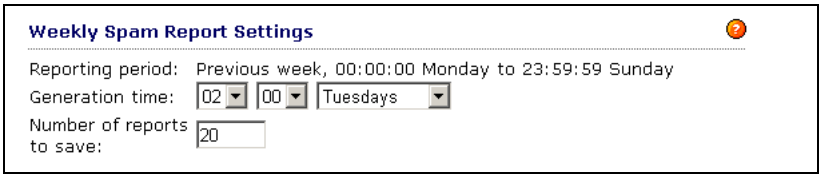
1. Open the Scheduled Reports screen by clicking **Spam Reports > Scheduled** in the left navigation panel.
2. Click **Settings** to the right of **Daily reports** to configure daily reporting.



   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.

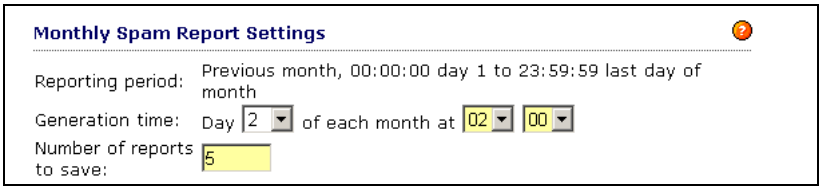
3. Click **Settings** to the right of **Weekly reports** to configure weekly reporting.



   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.

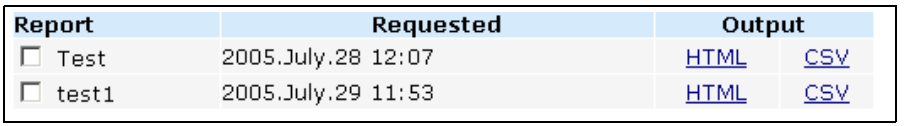
---

   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**.



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

Installation-related

C Runtime DLL (msvcrt.dll) 6.0 required

The Remote Installer/Uninstaller program called by the installation program requires C runtime DLL (msvcrt.dll) to be version 6.0 or newer. If the version of msvcrt.dll on the target machine is less than 6.0, the following error is returned:

```
C runtime DLL (msvcrt.dll) version too old
```

Run VC6RedistSetup_enu.exe from the \MSRedist folder on the disk or the location where you unpacked the installation files and re-run Setup.

Note: This issue primarily affects servers that are running Windows NT 4.0, not Windows 2000 or 2003.

Console cannot be viewed after installing Microsoft Proxy 2.0

Installing Microsoft® Proxy 2.0® prevents the default Web site from functioning correctly. A workaround is to create a second Web site and install the Common CGI filter on this Web site.

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, choose **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/default.asp`

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:

```
solutionbank.trendmicro.com/solutions/solutionSearch.asp
```

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 (in c:\Program Files) 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:

```
\Trend\InterScan MSS\ISNTSMTP\mqueue\
```

The retry queue is where undeliverable messages are kept pending retry:

```
\Trend\InterScan MSS\ISNTSMTP\bmqueue\
```

The postpone queue is where messages are stored temporarily as a result of a postpone filter action:

```
\Trend\InterScan MSS\ISNTSMTP\postpone\
```

To configure these directories, see *Mail processing queue directories* starting on page 3-11.

eManager, virus and program logs

Many modules in InterScan MSS write log information for troubleshooting purposes to the following folder:

```
\Trend\InterScan MSS\ISNTSMTP\logs\
```

For more information, see *Log maintenance* starting on page 3-16.

Default quarantine area

There is one default quarantine area established after program installation. In addition, multiple quarantine directories can be defined in different locations:

```
\Trend\InterScan MSS\IsntSmtp\quarantine
```

To change the quarantine directory, see *Managing quarantine areas* starting on page 4-12.

Badmail

Undeliverable messages can also be saved in this directory after the retry period has elapsed—see *Undeliverable messages (Badmail folder)* starting on page 3-32. A non-delivery receipt (NDR) is forwarded to the sender of a message that has been moved to the Badmail folder.

```
\Trend\InterScan MSS\isntsmtp\badmail
```

Note: This directory is not configurable.

Temporary folder

All application-generated temporary files are stored in the temporary folder:

```
\Trend\InterScan MSS\isntsmtp\temp\
```

Note: This directory is not configurable.

Delivery pickup folder

The **Quarantine Area** and the **Retry Queue Viewer** have a feature called **Deliver now**. Messages selected for "deliver now" are moved to this folder. The InterScan MSS service has dedicated threads that pick up the messages in this folder and deliver them immediately. See *Managing quarantine areas* starting on page 4-12 and *Viewing the Retry queue* starting on page 3-31 for more information.

```
\Trend\InterScan MSS\isntsmtp\pickup_deliver
```

Note: This directory is not configurable.

Scan pickup folder

Messages selected to be reprocessed from the **Quarantine Area** are placed in the pickup_scan folder for reprocessing. InterScan MSS has dedicated threads that pick up messages in this folder and place them in the scan queue. See *Using quarantine areas* starting on page 4-12 for more information.

```
\Trend\InterScan MSS\isntsmtp\pickup_scan
```

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** > **General**> **Notification** page. See *Notification settings* starting on page 3-10 for more information.

```
\Trend\InterScan MSS\isntsmtp\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.
- %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 that was attached to this message, %FILENAME%, was
found to be 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 that was attached to this message, resume.doc, was
found to be 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, the priority of the routes is calculated to determine which policy (that is, the one with the highest route priority) is applied 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 is matched 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 messages are analyzed, every email address is assigned a weight. Every sender and recipient pair (a “route”) is also given a weight 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

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 amonmainexe.exe to coordinate the information. Another adaptor DLL, amonadaptordll.dll (pre-defined in isntmtp.ini) invokes this program.

The settings in the isntsmtp.ini are:

[Plugin_Adapter]

Adapter_1=IsntPOP3Adapter.dll

Adapter_2=AmonAdaptorDll.dll

When InterScan MSS starts, each plugin listed under the Plugin_adaptor section is loaded.

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 \Trend\imss\isntsmtp.
   - 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**.

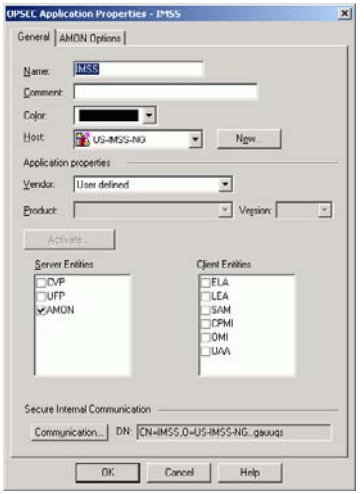


FIGURE C-3. OPSEC™ application properties screen

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 \trend\imss\isntmtp, 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**.

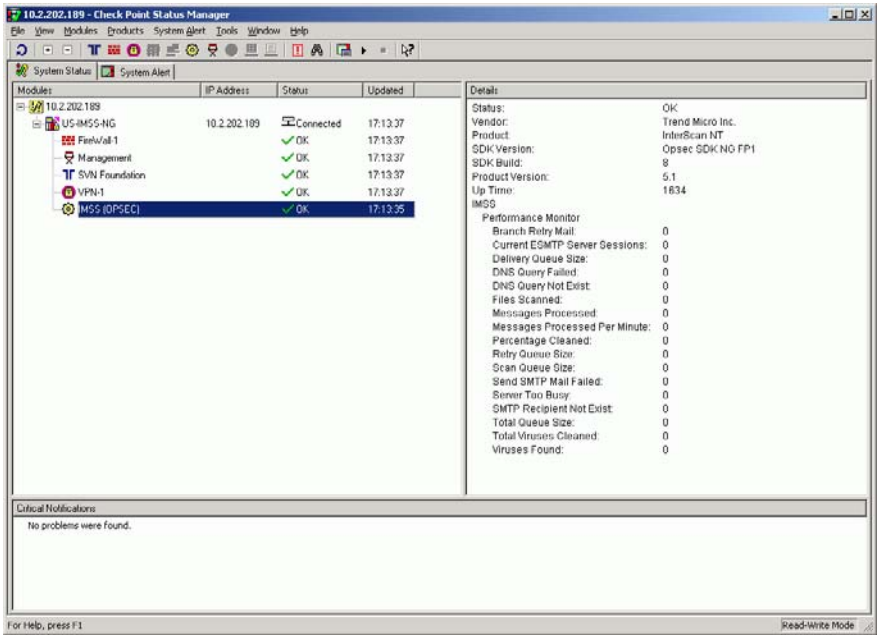


FIGURE C-4. Check Point™ Status Manager screen

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 Microsoft® Windows® Task Manager

You can also verify that the AMON server is working by using the **Windows Task Manager**.

To verify AMON status:

1. After InterScan MSS starts: find the amonmainexe.exe in the **Process** tab of the **Windows Task Manager**.
2. While InterScan MSS is stopped: click **Services** in the control panel to determine that the amonmainexe.exe. process has stopped.

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 categories 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

To install the agent, log on to Control Manager and open the console.

1. In the menu bar, click **Products** and in the navigation panel, click **Add/Remove Product Agents**.

FIGURE C-1. Control Manager main console

2. Under **Remote Agent Setup program**, click **Use this** next to **for obtaining, installing, and removing Control Manager agent-update packages** to download and save **RemoteInstall.exe**; double-click this file.
3. In the **Trend Control Manager Agent Setup** screen (Figure C-2.), you will see the following buttons:
   - **Install**
   - **Uninstall**
   - **Add/Update package**

   To add or update an agent package into the Control Manager server, click **Add/Update package**.

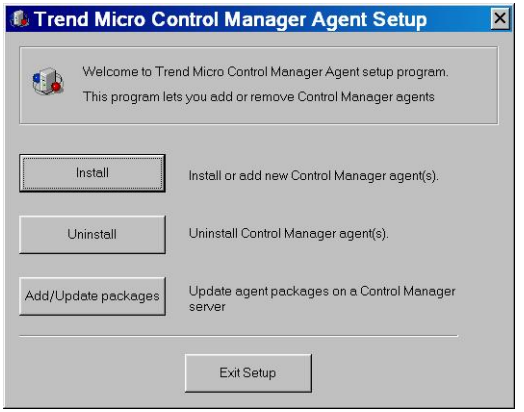


FIGURE C-2. Control Manager Agent setup

4. In the **Trend Micro Control Manager Agent Package Update** screen, in **Host**, enter a Control Manager server IP address. In **File**, type *RemoteInstall.xml* and type the path where this file can be found in the InterScan MSS agent package.

   If you do not know the exact path of the .xml file, click **Browse** to locate it. Once you have located this file, click **Open**. This file uploads the agent package to the Control Manager server. Click **Next**.

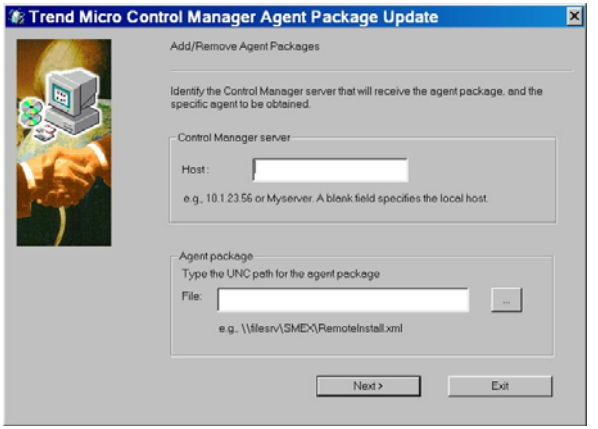


FIGURE C-3. Control Manager Agent package update screen

5. **Agent Package Information** displays information about the agent package. On the lower right side is information about the agent you are going to upload; on the lower left side is information about the existing agent. This information cannot be modified. Click **Upload**.
6. In the **Agent Import** pop-up window, if the agent was successfully updated, click **OK**. You will be prompted about updating another package. If you click **Yes**, the agent installation process is repeated; if you click **No**, you are returned to the **Trend Micro Agent Setup** screen. Click **Install**.

FIGURE C-4. Control Manager Agent welcome screen

7. In **Trend Micro Control Manager Agent Setup -- Welcome!**, click **Next** to start the process. When the **License Agreement** is displayed, read it and click **Next** to signify your agreement. In the next screen, select the agent you want to install (for example, InterScan Message Security Suite (English) V5.5)) and click **Next**.
8. In **Step 1 of 5**, type the appropriate information into the following fields:
   - **Host name**
   - **User name**
   - **Password**

   Click **Next**.
9. In **Step 2 of 5**, all the agents that exist in the Control Manager server are displayed. Select an agent and click **Next**. In the **Trend Micro Agent Server Selection** screen, select the servers to which InterScan MSS will install. You can do a remote or a local install.

To select a server, in the left pane, highlight the server and click **Add >>**. You can also type the server name in the field in the middle of the screen and click **Add>>** and click **Next**.

10. Log on to the selected servers by typing your administrator credentials. For servers that require different logon credentials, **Setup** displays the **Server Logon** screen again. After you log on, **Setup** displays a list of selected servers. Click **Next** and click **Next** again on the following screen.
11. Type an Administrator, Power User, Operator, or the root account on the Control Manager server for the **User ID**. Be sure to maintain this account. If this account is deliberately or accidentally deleted, you can no longer manage the agent.

Note: When installing agents, we recommend that you use the root account.

This **Entity name** is used to identify the product agent in the Control Manager server console directory.

12. When **Finished analyzing the servers** appears in a pop-up window, click **OK**. The installation process has verified that the servers exist and are working properly.You are now ready to install the agent.
13. In **Trend Micro Control Manager Agent Setup**, type the user ID for the Control Manager server and click **Next**. In **Setup Control Manager Agent**, type your User ID and click **Next**. The **Entity Name** is unavailable.
14. The **Setup Message Routing Path** is divided into two parts:
    - **Incoming messages**
    - **Outgoing messages**

    a. The default option is **any host**. If you have a firewall, you can choose **IP port forwarding** or **proxy server**.

    b. In **Route to forwarding messages**, select **direct server** and click **Next**.

    You are returned to the Control Manager console. In the navigation panel, choose **Products** > **Add/Remove Product Agent**.

FIGURE C-5. Add/Remove Product Agents screen

15. Click **Public encryption key**. Click the right mouse button and select **Save Target as**. In the **Register with Control Manager,** locate the *E2EPublic.dat* file and click **Next**.
16. Click **Import**.

    This information lets the agent know where the Control Manager server is and what type of communication to use.
17. In **Trend Micro Agent Setup-- Installing Agent**, the agent installation is started. When the installation has successfully completed, in the **Control Manager Agent Setup** screen, a **Finished installing agent message is displayed.** Click **OK** and then click **Next**.

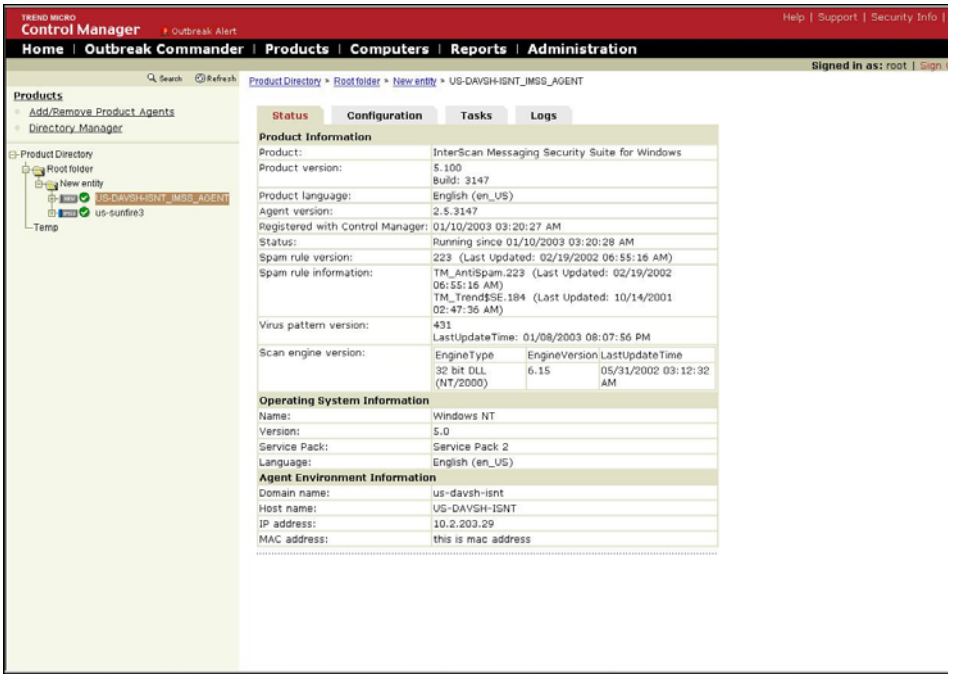


FIGURE C-6. Status of the Product Agent in Control Manager

18. When prompted to install additional agents, click **Yes** or **No**. Click **Finish** to return to the Control Manager console.

Removing the agent

1. Click **RemoteInstall.exe** and click **Uninstall** in the **Trend Micro Control Manager Agent Setup** screen. The **Trend Micro Control Manager Agent Uninstall -- Welcome!** screen is displayed. Click **Next**.
2. Enter your **hostname** and **password** and click **Next**. In the **Trend Micro Control Manager Agent Setup** screen, select the agent you want to remove and click **Uninstall**. Click **Next**.

3. The **Trend Micro Control Manager Server Selection** screen appears. From the list in the navigation panel, select the servers from which you want to remove the Control Manager agent and click **Next**. You can also type the server name in the field in the middle of the screen and click **Add**.
4. Enter the Administrator credentials for the selected servers. To log on multiple servers with the same account, select **Retain user name and password after logging on**.

   For servers that require different logon credentials, **Setup** displays the **Server Logon** screen again. After the logon process, **Setup** displays a list of selected servers. Click **Next**, and in the following screen, click **Next**.

   The **Entity name** is used to identify the product agent in the Control Manager server console directory.
5. When the **Finished analyzing servers** pop-up window appears, click **Next** and in the next screen, click **Uninstall**. When you see the **Finished Removing Agent** message in the pop-up window, click **OK** and you are returned to the Control Manager's main console.

Index

W

Z

Trend Micro Incorporated
10101 N. De Anza Blvd
Cupertino, CA., 95014 USA
www.trendmicro.com

For Sales:
Tel: +1-800-228-5651 (U.S. and Canada)
Tel: +1-408-257-1500 (outside the U.S. and Canada)
Fax: +1-408-257-2003

Item Code: MSEM51380/30620