Configuring SMTP and POP3 Mail Traffic

This chapter describes additional configuration required to detect security risks such as spyware or to add an organizational disclaimer to incoming and outgoing messages, and includes the following sections:

Default Mail Scanning Settings

Table 3-1 lists the mail configuration settings, and the default values that are in effect after installation.

Table 3-1 Default Mail Scanning Settings

Feature	Default Setting
SMTP scanning for incoming and outgoing mail	Enabled using All Scannable Files as the scanning method.
POP3 scanning	Enabled using All Scannable Files as the scanning method.
SMTP and POP3 scanning message filter (reject messages larger than a specified size)	Enabled to reject messages larger than 20 MB.
SMTP message rejection (reject messages with recipients higher than a specified number)	Enabled to reject messages addressed to more than 100 recipients.

Table 3-1 Default Mail Scanning Settings (continued)

Feature	Default Setting
SMTP and POP3 compressed file handling for incoming and outgoing mail	Configured to skip scanning of compressed files when one of the following is true: • Decompressed file count is greater than 200. • Decompressed file size exceeds 20 MB. • Number of compression layers exceeds three. • Decompressed or compressed file size ratio is greater than 100 to 1. • Compressed files exceed specified scanning criteria.
SMTP incoming and outgoing messages POP3 messages in which malware is detected	Clean the message or attachment in which the malware was detected. If the message or attachment is uncleanable, delete it.
SMTP incoming and outgoing messages POP3 messages in which spyware or grayware is detected	Allows files to be delivered.
SMTP incoming and outgoing messages POP3 notification when malware is detected	An inline notification is inserted in the message in which the malware was detected, which states: `%VIRUSNAME% was detected in the file (%FILENAME%). The following action has been taken:%ACTION%`
Password-protected SMTP and POP3 e-mail messages	Allows files to be delivered without scanning.

These default settings give you some protection for your e-mail traffic after you install Trend Micro InterScan for Cisco CSC SSM. You may change these settings. See the online help for more information about these selections before making e-mail changes.

To obtain the maximum protection for your e-mail traffic, additional configuration settings are available that you may want to update. If you purchased the Plus License, which entitles you to receive anti-spam and content filtering functionality, you must configure these features.

Defining Incoming and Outgoing SMTP Mail

When an e-mail message is addressed to multiple recipients, one or more of which is an incoming message (addressed to someone within the same organization with the same domain name) and one of which is outgoing (addressed to someone in a different organization with a different domain name), the incoming rules apply. For example, a message from psmith@example.com is addressed to jdoe@example.com and gwood@example.net.

The message from psmith to jdoe and gwood is treated as an incoming message for both recipients, although gwood is considered an “outgoing” recipient.

You should set scanning to the Scan all option for incoming SMTP messages, and scanning to the IntelliScan option for outgoing messages. Make sure that you enable spyware or grayware detection for incoming messages only.

Enabling SMTP and POP3 Spyware and Grayware Detection

Grayware is a category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data; however, it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.

To detect spyware and other forms of grayware in your e-mail traffic, you must configure this feature on the SMTP Incoming Message Scan/Target, SMTP Outgoing Message Scan/Target, and POP3 Scanning/Target windows according to the following steps:

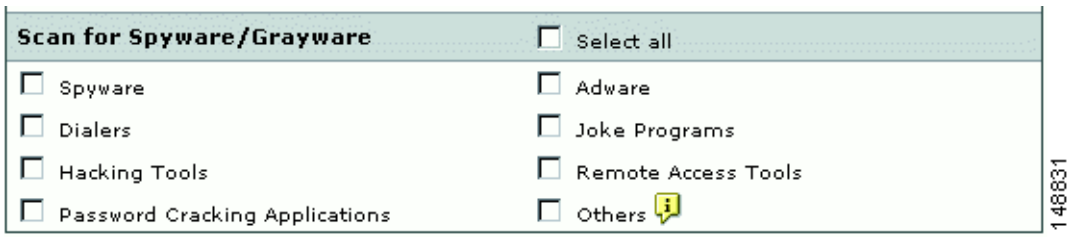
Step 1 To display the SMTP Incoming Message Scan/Target window, choose **Configuration > Trend Micro Content Security > Mail** in ASDM and click the **Configure Incoming Scan** link.

Step 2 To display the SMTP Outgoing Message Scan/Target window, choose **Configuration > Trend Micro Content Security > Mail** in ASDM and click the **Configure Outgoing Scan** link.

Step 3 To display the POP3 Scanning/Target window, in the CSC SSM console, choose **Mail (POP3) > Scanning > POP3 Scanning/Target**.

Step 4 In the Scan for Spyware/Grayware section of these windows (shown in Figure 3-1), choose the types of grayware you want detected by Trend Micro InterScan for Cisco CSC SSM. See the online help for a description of each type of grayware listed.

Figure 3-1 Spyware and Grayware Scanning Configuration



Step 5 Click **Save** to enable the new configuration.

Reviewing SMTP and POP3 Notifications

This section describes notification settings and includes the following topics:

- Types of Notifications, page 3-4
- Modifying Notifications, page 3-4

If you are satisfied with the default notification setup, no further action is required. However, you might want to review the notification options and decide whether you want to change the defaults. For example, you may want to send a notification to the administrator when a security risk has been detected in an e-mail message. For SMTP, you can also notify the sender or recipient.

You may also want to tailor the default text in the notification message to something more appropriate for your organization.

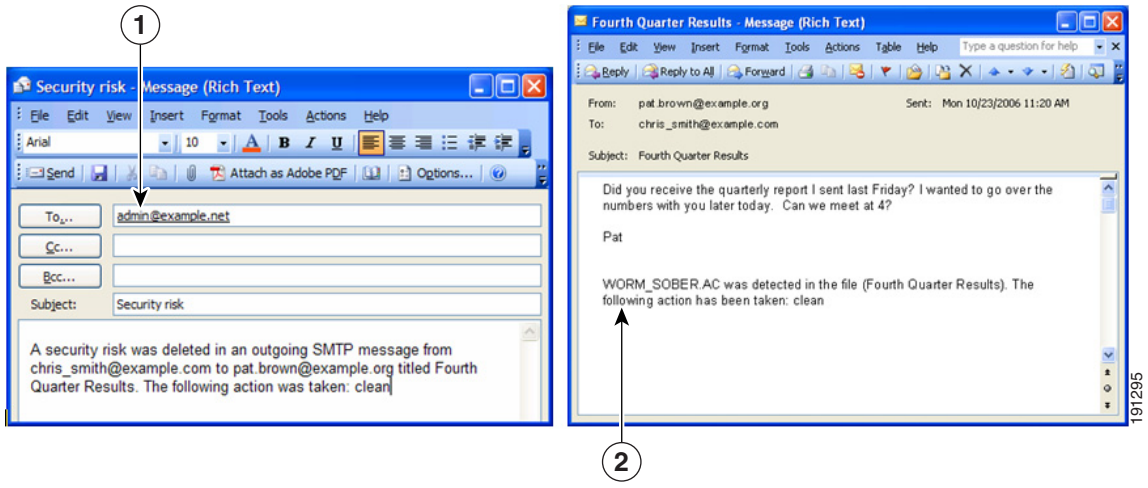
To review and reconfigure e-mail notifications, go to each of the following windows in the CSC SSM console:

- Mail (SMTP) > Scanning > Incoming > SMTP Incoming Message Scan/Notification
- Mail (SMTP) > Scanning > Outgoing > SMTP Outgoing Message Scan/Notification
- Mail (POP3) > Scanning > POP3 Scanning/Notification

Types of Notifications

There are two types of notifications available in e-mail traffic: e-mail notifications and inline notifications, as shown in Figure 3-2.

Figure 3-2 Examples of Notifications



1	E-mail notification	2	Inline notification

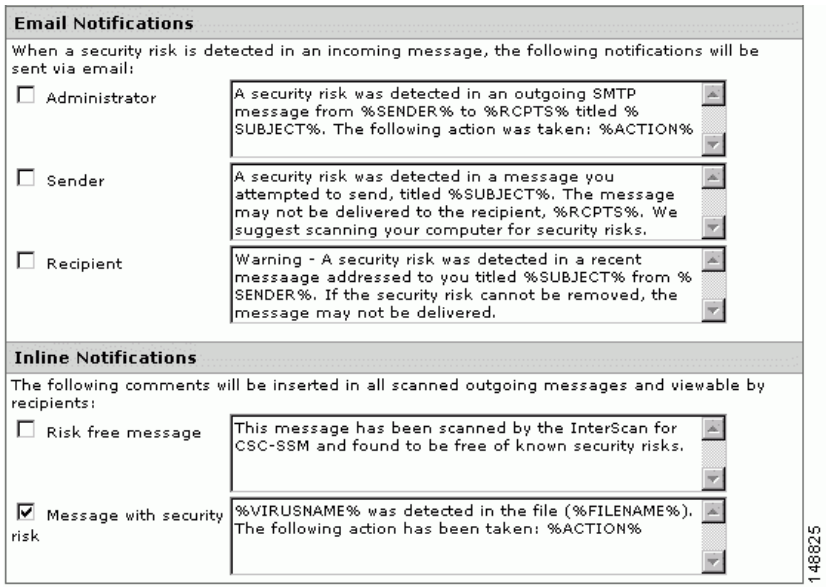
Notifications use variables called *tokens* to provide information that makes the notification more meaningful. For example, a token called **%VIRUSNAME%** is replaced with the text `WORM_SOBER.AC` in the inline notification example on the right.

For more information about tokens, see the online help topic, "Using Tokens in Notifications."

Modifying Notifications

To send a notification to additional recipients, or to change the default text of the notification message that is sent when an event occurs, go to the applicable window to update the settings. For example, Figure 3-3 shows the notification options on the Mail (SMTP) > Scanning > Outgoing > SMTP Outgoing Message Scan/Notification window.

Figure 3-3 Configure Notifications for Outgoing SMTP Messages



By default, the only notification is an inline notification to the message recipient, which means neither the sender nor the administrator of the originating organization is aware that a security threat has been detected and cleaned.

To make changes to these notifications:

Step 1 In the Email Notifications section of the window, select additional people to receive an e-mail notification.

Step 2 In the Inline Notifications section of the window, choose one of the listed options, neither, or both.

Step 3 Highlight the existing text and type your own message in the field provided.

Step 4 Click **Save** when you are finished.

Configuring SMTP Settings

Review the configuration settings available in the Mail (SMTP) > Configuration > SMTP Configuration window. The SMTP Configuration window contains the following four tabs:

- Message Filter
- Disclaimer
- Incoming Mail Domain
- Advanced Settings

Note These settings apply to SMTP messages only.

To configure settings in this window, perform the following steps:

Step 1 In the Message Filter tab, Trend Micro InterScan for Cisco CSC SSM is already configured to reject messages larger than 20 MB and messages addressed to more than 100 recipients. These settings protect you from an assault on your network that consumes CPU time while your e-mail server tries to handle large, bogus messages addressed to hundreds of recipients. The default settings are recommended, and if you want to continue to use them, no action is required on this window.

Step 2 In the Message Filter tab of the SMTP Configuration window, you may add an organizational disclaimer that appears at the beginning or end of SMTP messages. Check **Add this disclaimer** to enable this feature, or leave this option blank if you do not want to use this feature. To customize the disclaimer text, highlight it and redefine the message.

Step 3 In the Incoming Mail tab of the SMTP Configuration window, you can define additional incoming e-mail domains to do the following:

- Scan for viruses and other threats.
- Provide anti-spam functions.
- Perform content-filtering.

The Incoming mail domains field should already contain the incoming e-mail domain name you entered in the Host Configuration installation window during installation. If you have additions, enter the top-level domain (tld) name only. For example, enter only **example.com**; exclude subsidiary domains such as example1.com, example2.com, and so on. If there are no other incoming domains, no further action is needed.

Step 4 The Advanced Settings tab of the SMTP Configuration window contains fields that allow you to do the following:

- Set a more aggressive (or permissive) timeout for messages that appear to be from an attacker.
- Enable settings that place selected, temporary restrictions on the SMTP traffic. If you suspect you may be under attack, these restrictions make it more difficult for the traffic that has the characteristics of a suspicious message from an attacker to move through a system because you have performed the following:
  - Set a shorter timeout for sending an e-mail (often an e-mail that takes longer to send is part of an intentional attempt to consume resources).
  - Limited the allowed number of errors triggered, indicative of someone resending a message over and over.
  - Limited the number of times the sender resets the conditions for attempting to send the same e-mail.

Step 5 After you make changes, click **Save** to activate your updated SMTP configuration.

Enabling SMTP and POP3 Spam Filtering

You must configure the SMTP and POP3 anti-spam feature.

Note This feature requires the Plus License.

To configure the anti-spam feature, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Mail window in ASDM, click the **Configure Anti-spam** link to display the SMTP Incoming Anti-spam window.

Step 2 In the CSC SSM console, choose **Mail (POP3) > Anti-spam > POP3 Anti-spam** to display the POP3 Anti-spam window.

Step 3 For each of these windows, click **Enable**.

Step 4 Reset the anti-spam threshold to **Medium** or **High** if you do not want to use the default value.

Tip You might want to adjust this setting at a later time, after you have some experience with blocking spam in your organization. If the threshold is too low, a high incidence of spam occurs. If the threshold is too high, a high incidence of false positives (legitimate messages that are identified as spam) occurs.

Step 5 In the Approved Senders section of the SMTP Incoming Anti-spam and POP3 Anti-spam/Target windows, add approved senders. Mail from approved senders is always accepted without being evaluated.

Note Approved senders that you have added and saved in either window appear in both windows. For example, if you add yourname@example.com to the Approved Senders list on the POP3 Anti-spam window. Open the SMTP Incoming Anti-spam window. The address for yourname@example.com has already been added to the list of Approved Senders on the SMTP Incoming Anti-spam window.

You can create the Blocked Senders list in either window; however, the list appears in both windows.

Step 6 In the Blocked Senders section of the SMTP Incoming Anti-spam and POP3 Anti-spam/Target windows, add the blocked senders. Mail from blocked senders is always rejected. Blocked senders that you have added and saved in either window appear in both windows.

Step 7 Configure the action for messages identified as spam on the SMTP Incoming Anti-spam and POP3 Anti-spam/Action windows. Choose one of the following options:

- Stamp the message with a spam identifier, such as “Spam:” and deliver it anyway. The spam identifier acts as a prefix to the message subject (for example, “Spam:Designer luggage at a fraction of the cost!”).
- Delete the message.

Step 8 Click **Save** to activate the new anti-spam configuration settings.

Enabling SMTP and POP3 Content Filtering

You must configure the SMTP and POP3 content filtering feature.

Note This feature requires the Plus License.

To configure the content filtering feature, perform the following steps:

Step 1 On the Configuration > Trend Micro Content Security > Mail window in ASDM, click the **Configure Incoming Filtering** link to display the SMTP Incoming Content Filtering/Target window.

Step 2 On the Configuration > Trend Micro Content Security > Mail window in ASDM, click the **Configure Outgoing Filtering** link to display the SMTP Outgoing Content Filtering/Target window.

Step 3 On the CSC SSM console, choose **Mail (POP3) > Content Filtering > POP3 Content Filtering/Target** to display the POP3 Content Filtering/Target window.

Step 4 For each of these windows, click **Enable**.

Step 5 Decide whether to use message size filtering criteria, and if so, set the parameters in the Message size is field. For example, if you specify message filtering for messages and attachments greater than 5 MB, messages with attachments less than 5 MB are not filtered. If you do not specify a message size, all messages are filtered, regardless of their size.

Step 6 In the Message Subject and Body section of the windows, specify words that if present in the message subject or body, trigger content filtering.

Step 7 In the Message Attachment section of the windows, specify characters or words that if present in the attachment name, trigger content filtering. You can also choose content filtering by file types in this section of the window. For example, if you choose **Microsoft Office** file types for filtering, attachments created with Microsoft Office tools are filtered for content.

Step 8 On each of these windows, click the **Action** tab to specify what action triggers content filtering. For e-mail messages, the options are as follows:

- Delete messages that violate one of the content filtering policies.
- Deliver messages anyway.

For attachments, the options are as follows:

- Allow violating attachments to pass. In this case, do not make any changes in the For messages that match the attachment criteria section of the window.
- Delete the attachment and insert an inline notification in the message body.

Step 9 On each of these windows, click the **Notification** tab to specify whether a notification is sent to the administrator for a content filtering violation. For SMTP, you can also notify the sender or recipient. Change the default text in the notification message by selecting it and redefining the message.

Step 10 Click **Save** to activate content filtering according to the new configuration settings.

Enabling Network Reputation Services

In addition to filtering spam on the basis of content, CSC SSM provides Network Reputation Services (NRS), which allow you to determine spam based on the reputation of the originating MTA, which off-loads the task from the CSC SSM server. With NRS enabled, all inbound SMTP traffic is checked by the IP databases to see whether the originating IP address is clean or it has been black-listed as a known spam vector.

About RBL+ and QIL

The Realtime Blackhole List (RBL+) is a database that tracks the reputation of about two billion IP addresses. IP addresses that have been consistently associated with the delivery of spam messages are added to the database and rarely removed. The Quick IP Lookup (QIL) list is another database for tracking the reputation of IP addresses, but with this database, IP addresses are added and removed more frequently and thus, can be considered more current.

When an IP address is found in either database, NRS "marks" the connection and CSC SSM behaves according to the settings that you have selected.

For example, an MTA has been hijacked or an open relay exploited and used by a third party to deliver spam messages. The system administrator may discover the exploit after a brief period of time and correct it. Nevertheless, during this period of time, millions of spam messages are being and have been sent by the server. The tainted IP address may be added to the QIL database after only a few reports of spam, but then removed after the reports have subsided. On the other hand, because it takes longer for an IP address to be added to the RBL+, many that are only temporarily problematic (but nonetheless responsible for millions of spam) are not flagged by RBL+. After these IP addresses have been added to the RBL+, however, it is more difficult to remove them from the database.

Note There is a higher degree of certainty that IP addresses in the RBL+ are confirmed spam MTAs.

Both services are applied to the message before the message is delivered to your MTA, freeing it from the overhead of processing complex heuristics and analysis and routing the mail at the same time.

To enable and configure NRS filtering, perform the following steps:

Step 1 On the CSC SSM console, choose **Mail (SMTP) > Network Reputation Services** to open the Target window.

Step 2 Click **Enable**.

Step 3 Choose the level of service you want to use: High or Low. The high service level uses both the RBL+ and Quick IP Lookup services to check the reputation of the MTA from which the e-mail is received.

Step 4 In the Approved IP Address field, add the IP address or a range of IP addresses for any PCs you want to exempt from the lookup service.

Step 5 Click the **Action** tab to make that page active, and then choose the action you want the CSC SSM to take on messages found to match an entry in the RBL+ or QIL database. The available actions are as follows:

- Intelligent action—Spam messages are rejected at the MTA with a brief message.
- Connection closed with no error**—**Spam messages are rejected, but no message is sent.

Note This action may trigger a series of automatic retries on the part of the originating MTA, and can increase traffic volume.

- Detect, log, then pass—Spam incidents are logged and then delivered to the intended recipient, and other scanning rules are applied. This action is typically used only for troubleshooting.