CHAPTER 3

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	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	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 500. • 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	Cleans the message or attachment in which the malware was detected. If the message or attachment is uncleanable, delete it (SMTP only) or replace with notification.
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 settings 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 “All scannable files” option for incoming SMTP messages, and scanning to the IntelliScan option for outgoing messages. You should set IntelliTrap to scan incoming messages, although it can also be configured to scan outgoing messages. Make sure that you enable spyware or grayware detection for incoming messages only.

About IntelliScan™

Most antivirus solutions today offer you two options in determining which files to scan for potential risks. Either all files are scanned (the safest approach), or only those files with certain file name extensions (considered the most vulnerable to infection) are scanned. But recent developments involving files being “disguised” through having their extensions changed has made this latter option less effective. IntelliScan is a Trend Micro technology that identifies a file’s “true file type,” regardless of the file name extension.

Note IntelliScan examines the header of every file, but based on certain indicators, selects only files that it determines are susceptible to virus infection.

True File Type

When set to scan true file type, the scan engine examines the file header rather than the file name to ascertain the actual file type. For example, if the scan engine is set to scan all executable files and it encounters a file named “family.gif,” it does not assume the file is a graphic file and skip scanning. Instead, the scan engine opens the file header and examines the internally registered data type to determine whether the file is indeed a graphic file, or, for example, an executable that has been deceptively named to avoid detection.

True file type scanning works in conjunction with Trend Micro IntelliScan, to scan only those file types known to be of potential danger. These technologies can mean a reduction in the overall number of files that the scan engine must examine (perhaps as much as a two-thirds reduction), but it comes at the cost of potentially higher risk.

For example, .gif and .jpg files make up a large volume of all web traffic, but they cannot harbor viruses, launch executable code, or carry out any known or theoretical exploits. However, this does not mean that they are entirely safe. It is possible for a malicious hacker to give a harmful file a “safe” file name to smuggle it past the scan engine and onto the network. The file could not run until it was renamed, but IntelliScan would not stop the code from entering the network.

Note For the highest level of security, Trend Micro recommends scanning all files.

About IntelliTrap™

IntelliTrap works in real-time to detect potentially malicious code in compressed files that arrive as e-mail attachments. This feature is turned off by default. Enabling IntelliTrap allows CSC SSM to take user-defined actions on infected attachments, and to send notifications to senders, recipients, or administrators.

Enable IntelliTrap by checking the check box in the IntelliTrap sections of the following locations:

- Mail (SMTP) > Scanning > Incoming or Outgoing/Target

- Mail (POP3) > Scanning/Target

When IntelliTrap detects malware, the users can choose one of the following actions:

- Allow files to be delivered
- Delete files

IntelliTrap technology is heuristically based, which allows it to detect previously unknown or new viruses. However, there are always a certain number of false positives. For this reason, Trend Micro recommends using the "Allow files to be delivered" action setting when you use this feature. With the action setting "Delete files," the only way to recover the file is to have the sender resend the e-mail message with the attachment.

The action settings are available at the following locations:

- Mail (SMTP) > Scanning > Incoming or Outgoing/Action
- Mail (POP3) > Scanning/Action

Notifications can be configured at the following locations:

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

For more information about Notifications, see Reviewing SMTP and POP3 Notifications, page 3-5.

To update the IntelliTrap Pattern and IntelliTrap Exception Pattern, check the check box for each component on the Summary page and click **Update,** or set up schedule updates by choosing **Update > Scheduled**. For more information about scheduled updates, see Scheduled Update, page 5-2.

Enabling SMTP and POP3 Spyware and Grayware Detection

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:

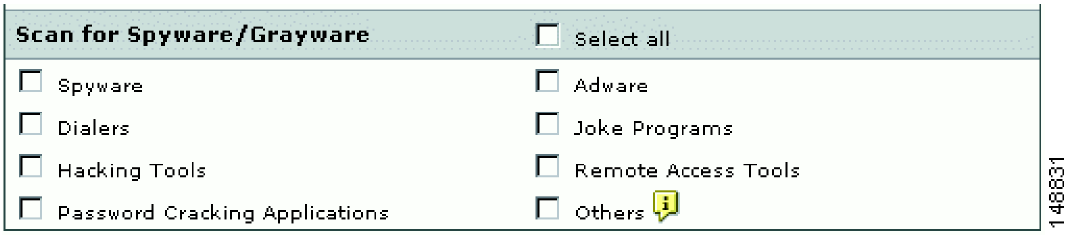
Step 1 To display the SMTP Incoming Message Scan/Target window, choose **Configuration > Trend Micro Content Security > Mail** in ASDM and click the **Configure Incoming Scan** link.

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



Scan for Spyware/Grayware	□ Select all
□ Spyware	□ Adware
□ Dialers	□ Joke Programs
□ Hacking Tools	□ Remote Access Tools
□ Password Cracking Applications	□ Others

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 3-5
- Modifying Notifications, page 3-6

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.

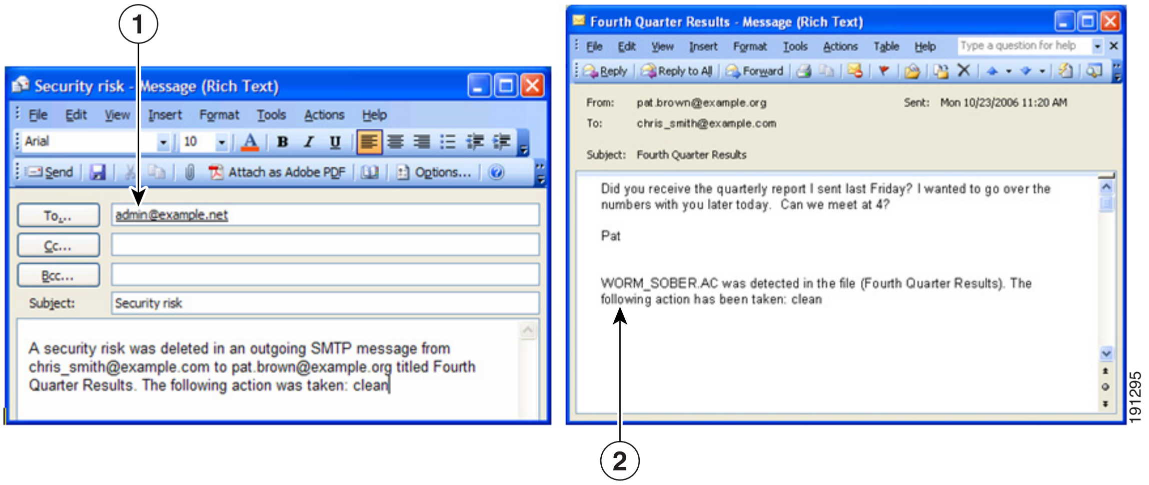
To review and reconfigure e-mail notifications, go to each of the following windows in the CSC SSM console:

- 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
Security risk - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Arial 10
Send
Attach as Adobe PDF
Options...
Fourth Quarter Results - Message (Rich Text)
File Edit View Insert Format Tools Actions Table Help
Type a question for help
Reply Reply to All Forward
2
191295

To... admin@example.net
Cc...
Bcc...
Subject: Security risk

A security risk was deleted in an outgoing SMTP message from chris_smith@example.com to pat.brown@example.org titled Fourth Quarter Results. The following action was taken: clean

From: pat.brown@example.org Sent: Mon 10/23/2006 11:20 AM
To: chris_smith@example.com
Subject: Fourth Quarter Results

Did you receive the quarterly report I sent last Friday? I wanted to go over the numbers with you later today. Can we meet at 4?

Pat

WORM_SOBER.AC was detected in the file (Fourth Quarter Results). The following action has been taken: clean

1	E-mail notification	**2**	Inline notification

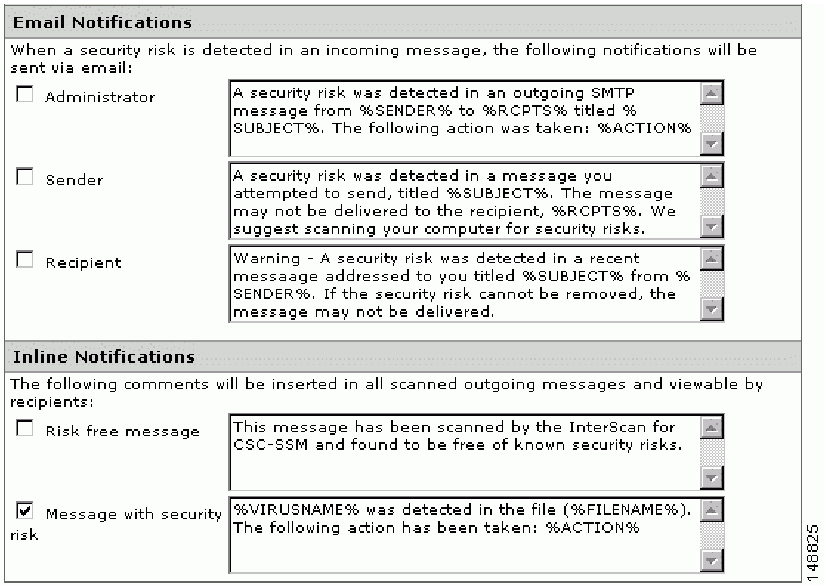
Notifications use variables called *tokens* to provide information that makes the notification more meaningful. For example, a token called %VIRUSNAME% is replaced with the text `WORM_SOBER.AC` in the inline notification example on the right.

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



Email Notifications

When a security risk is detected in an incoming message, the following notifications will be sent via email:

□ Administrator: A security risk was detected in an outgoing SMTP message from %SENDER% to %RCPTS% titled %SUBJECT%. The following action was taken: %ACTION%

□ Sender: A security risk was detected in a message you attempted to send, titled %SUBJECT%. The message may not be delivered to the recipient, %RCPTS%. We suggest scanning your computer for security risks.

□ Recipient: Warning - A security risk was detected in a recent messaage addressed to you titled %SUBJECT% from %SENDER%. If the security risk cannot be removed, the message may not be delivered.

Inline Notifications

The following comments will be inserted in all scanned outgoing messages and viewable by recipients:

□ Risk free message: This message has been scanned by the InterScan for CSC-SSM and found to be free of known security risks.

☑ Message with security risk: %VIRUSNAME% was detected in the file (%FILENAME%). The following action has been taken: %ACTION%

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, perform the following steps:

Step 1 In the Email Notifications section of the window, check the applicable check boxes provided to have additional people receive e-mail notifications.

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 Disclaimer tab of the SMTP Configuration window, you may add an organizational disclaimer that appears at the beginning or end of SMTP messages.

- To enable this feature, check one or both of the following check boxes:
  - Display disclaimer in all incoming e-mail messages.
  - Display disclaimer in all outgoing e-mail messages.

  Note Leave this option blank if you do not want to use this feature.

- Select the location of the disclaimer using the Location drop-down box.
- If needed, customize the disclaimer text by highlighting it and redefining the message.
- Click **Save**.

Step 3 In the Incoming Mail Domain 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.

- The **Enable SMTP TLS traffic pass-through mode** check box is disabled by default. This setting allows sending and receiving MTAs to communicate using the encrypted TLS protocol.

Caution SMTP e-mail messages delivered via TLS are not scanned or filtered by CSC SSM, and could allow malicious content to enter the network. Email Reputation still scans all SMTP e-mail messages for spam.

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 Anti-spam > Content Scanning/Target window.

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

Step 3 For each of these windows (SMTP and POP3), 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 Mail (SMTP) > Anti-spam > Content Scanning/Target or 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 Mail (POP3) > Anti-spam/Target window. Open the SMTP Anti-spam > Content Scanning/Target window. The address for yourname@example.com has already been added to the list of Approved Senders on the Mail (SMTP) > Anti-spam > Content Scanning/Target window.

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

Approved and blocked senders lists can also be imported. The imported file must be in a specific format. See the online help for instructions.

Step 6 In the Blocked Senders section of the Mail (SMTP) > Anti-spam > Content Scanning/Target and Mail (POP3) > Anti-spam/Target windows, add the blocked senders. Mail (spam and non-spam) 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.

a. Go to the **Mail (SMTP) > Anti-spam > Content Scanning/Action** tab, and select 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 message.

b. Go to the **Mail (POP3) > Anti-spam/Action** tab, and select 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!").
   - Replace with notification to inform the recipient that the mail was not delivered because it violated an anti-spam policy.

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 (SMTP Incoming and Outgoing, and POP3), 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:

a. Go to the **Mail (SMTP) > Content Filtering > Incoming or Outgoing/Action** tab, and select one of the following options:

- Delete messages (messages will not be delivered).
- Deliver messages anyway.

For attachments, select from the following options:

- 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.

b. Go to the **Mail (POP3) > Content Filtering/Action** tab, and select one of the following options:

For messages that match the filtering criteria:

- Replace with notification to inform the recipient that the mail was not delivered because it violated a content filtering policy.
- Deliver messages anyway.

For messages that match the attachment criteria, select from the following options:

- 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 Email Reputation

In addition to filtering spam on the basis of content, CSC SSM provides Email Reputation (ER) technology, which allow you to determine spam based on the reputation of the originating MTA. This off-loads the task from the CSC SSM server. With ER 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.

Note For Email Reputation Services to function properly, all address translation on inbound SMTP traffic must occur after traffic passes through the CSC SSM. If NAT or PAT takes place before the inbound SMTP traffic reaches the CSC SSM, CSC SSM will always see the local address as the originating MTA. ERS only blocks connections from suspect MTA public IP addresses, not private or local addresses. Therefore, customers using Email Reputation Services should not translate inbound SMTP connections before they are scanned by CSC SSM.

About Standard and Advanced Services

*Email Reputation Services — Standard (*ERS — Standard*)* service (formerly known as Realtime Blackhole List or 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.

Email Reputation Services — Advanced (ERS — Advanced) service (formerly RBL + and Quick IP Lookup or QIL combined) is a DNS, query-based service like Email Reputation Services Standard. At the core of this service is the standard reputation database, along with the dynamic reputation, real-time database. This service stops sources of spam while they are in the process of sending millions of messages.

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

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 dynamic reputation database (used by ERS — Advanced) 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 standard reputation database (used by ERS-Standard), many that are only temporarily problematic (but nonetheless responsible for millions of spam) are not flagged by the standard reputation database. After these IP addresses have been added to the standard reputation database, however, it is more difficult to remove them from the database.

Note There is a higher degree of certainty that IP addresses in the standard reputation database 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.

Enabling and Configuring ER

Note This feature requires the Plus License.

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

Step 1 On the CSC SSM console, choose **Mail (SMTP) > Anti-spam > Email Reputation** to open the Target window.

Step 2 Click **Enable**.

Step 3 Choose the level of service you want to use: Standard or Advanced. The Advanced service level uses both standard and dynamic reputation database 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 databases used by the standard or advanced service. 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.