The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright notice
Copyright © 2006 Symantec Corporation.
All rights reserved.
Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks
Symantec, the Symantec logo, Symantec TurnTide and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1
Contents

Chapter 1  Introduction
How Symantec Hosted Mail Security works .................................................5
About email filtering .........................................................................................6
Types of Email Actions ....................................................................................7
False positives and missed spam .....................................................................7
Reporting missed spam to Symantec ............................................................8
Reporting false positives to Symantec .........................................................8

Chapter 2  The Spam Quarantine Report
About the Spam Quarantine Report ...............................................................11
About the Spam Quarantine Summary ..........................................................14

Chapter 3  Using the console
Overview of the Symantec Hosted Mail Security Console .........................16
Setting or changing your password ...............................................................16
Requesting a password ................................................................................16
Resetting your password .............................................................................17
Changing your password .............................................................................18
Logging into the Symantec Hosted Mail Security Console .........................19
Managing your personal Message Quarantine ..............................................19
Selecting which email addresses to include .................................................20
Reviewing a single quarantined email ..........................................................20
Releasing multiple emails ............................................................................21
Deleting multiple emails ..............................................................................21
Adding senders to an Allow list from the Message Quarantine ..................22
Adding senders to a Deny list from the Message Quarantine .......................22
Maintaining Allow and Deny lists ...............................................................23
Adding a single sender to an allow or deny list ..........................................23
Adding multiple senders to an Allow or Deny list ......................................24
Removing senders from an Allow or Deny list ............................................25
Saving an Allow or Deny list to a file ..........................................................25
Configuring your preferences .......................................................................26
Turning spam filtering on or off ...................................................................27
Selecting spam email actions .......................................................................27
Selecting Spam Quarantine Report frequency ............................................28
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selecting Spam Quarantine Report content</td>
<td>29</td>
</tr>
<tr>
<td>Setting the time zone for your email processing</td>
<td>29</td>
</tr>
<tr>
<td>Choosing language filtering options</td>
<td>30</td>
</tr>
<tr>
<td>Maintaining your alias email addresses</td>
<td>30</td>
</tr>
<tr>
<td>When you add an alias email address</td>
<td>31</td>
</tr>
<tr>
<td>Converting a primary email address to an alias address</td>
<td>32</td>
</tr>
<tr>
<td>Deleting associated email addresses</td>
<td>32</td>
</tr>
<tr>
<td>Accessing the User Aliases settings</td>
<td>33</td>
</tr>
<tr>
<td>Selecting which email address is primary</td>
<td>33</td>
</tr>
<tr>
<td>Adding an alias email address</td>
<td>34</td>
</tr>
<tr>
<td>Deleting an alias email address</td>
<td>35</td>
</tr>
</tbody>
</table>
Introduction

This chapter includes the following topics:

- How Symantec Hosted Mail Security works
- About email filtering

How Symantec Hosted Mail Security works

Symantec Hosted Mail Security lets you manage your personal Message Quarantine for spam messages. Symantec Hosted Mail Security quarantines emails that are suspected to be spam in a safe location. Depending on the configuration of your hosted mail service, you will receive Spam Quarantine Reports or a text-based message via email on a regular basis notifying you that you have quarantined email.

You can manage your quarantined email using the Symantec Hosted Mail Security Console. You can log into the Symantec Hosted Mail Security Console using a Web browser or you can click a link in the Spam Quarantine Report or Spam Quarantine Summary.

Depending on your system’s configuration, you can perform any of the following tasks:

- Create or change your password for the Symantec Hosted Mail Security Console (“Logging into the Symantec Hosted Mail Security Console” on page 19)
- Log into the Symantec Hosted Mail Security Console (“Logging into the Symantec Hosted Mail Security Console” on page 19)
- Manage the emails in your quarantine area (“Managing your personal Message Quarantine” on page 19)
- Manage your personal Allow Sender and Deny Sender lists (“Maintaining Allow and Deny lists” on page 23)
■ Configure additional email addresses to be included in your Spam Quarantine Report ("Maintaining your alias email addresses" on page 30)

■ Configure settings controlling your Spam Quarantine Report and spam filtering ("The alias email address is deleted immediately." on page 35)

From the Spam Quarantine Report, you can perform most of the same actions that are available in the Symantec Hosted Mail Security Console ("The Spam Quarantine Report" on page 11).

**Note:** The administrator for your organization determines which features are available for you to use. This guide assumes that all the features are available and enabled. If you see a feature described in this manual that you cannot access, contact your administrator.

---

**About email filtering**

The administrator for your organization has configured the types of email filtering and resultant actions that will be applied to your email. Depending on the configurations, Symantec Hosted Mail Security will typically perform the following email filtering:

■ **Virus and Worm Scanning** – Symantec Hosted Mail Security determines whether an email’s attachment contains any known viruses or worms and if it does, performs the configured action on the email.

■ **Spam Blocking** – Symantec Hosted Mail Security analyzes the email to see if it is likely spam and, depending on the likelihood level, performs the configured action on the email.

■ **Content Filtering** – Symantec Hosted Mail Security analyzes the email to see if it violates configured content policies (for example, contains profanity, HTML links to images, or certain languages) and if it does, performs the configured action on the email.

■ **Attachment Filtering** – Symantec Hosted Mail Security analyzes the email’s attachment to see if it violates configured attachment policies (for example, exceeds a specified file size or is an executable program) and if it does, performs the configured action on the email.

■ **Additional filtering** – Symantec Hosted Mail Security performs any other email filtering as configured by the administrator (for example, filter “click-throughs” on hyperlinks in emails, use domain-level Allow Sender and Deny Sender lists, etc.).
Types of Email Actions

Based on the defined policy configuration, each email that violated the specified policy can have any of the following actions taken:

■ Do Nothing or Allow Delivery – The email is forwarded to your email address with no processing applied.

■ Quarantine – The email is added to the respective quarantine area and is not sent to your email address. If the email violated a spam policy, the email is reported in your Spam Quarantine Report. Quarantined emails can be viewed, deleted, and/or released to be sent to your email address. Be aware that you can manage only emails that were quarantined because of spam. You cannot access emails that were quarantined because of viruses, attachments, or content. Only the administrator can view and manage those emails.

■ Tag – The subject line of the email has a descriptive phrase (for example, “[SPAM]”) added to the beginning of the subject text and the email is sent to your email address.

■ Deny Delivery – The email is blocked automatically. Depending on the sending system’s configuration, you or the email sender may or may not be notified.

■ Strip Attachment – If the email had an attachment that violated attachment policies, this action causes that attachment to be removed from the email and the email is be sent to your email address. Text is inserted into the email notifying you that an attachment has been stripped. Only the attachment that violated the attachment policy is stripped.

■ Clean – If the email had an attachment that contained a virus or worm, this action attempts to remove the virus or worm and preserve the attachment. If the clean is successful, text is inserted into the email notifying you that an attachment had contained a virus and was cleaned.

False positives and missed spam

If you have received email that you feel should have been filtered, do the following

1. Check that the sending email address was not added to an Allow Sender list by either you or your administrator.

2. Confirm that you did not designate that your emails are not filtered for spam.
3 Confirm with your administrator that the policy settings in Symantec Hosted Mail Security have not been changed to allow these emails to bypass filtering (for example, the sender address has been added to the global Allow list, or the spam filtering feature has been turned off at the domain level).

**Reporting missed spam to Symantec**

You can submit spam or suspected spam messages that were not detected by the hosted mail security service to Symantec Security Response. Symantec engineers will analyze the message for spam characteristics and will issue updates to the spam filtering rules as needed.

You should submit the missed spam within 24 hours of when you received the message to ensure timely updates and to avoid analyzing messages for which updated rules have already been issued.

You can submit the missed spam to one of the following email addresses:

**North America**
Gsubmit@submit-1.brightmail.com

**Europe, Middle East, Africa**
eurosubmit@submit-23.brightmail.com

**Japan, Asia, Pacific Rim**
apacsubmit@submit-22.brightmail.com

---

**Note:** These addresses are for missed spam messages only. You must submit the message as an RFC-822 MIME-encoded attachment. You should include all header information, content, and attachments.

**Reporting false positives to Symantec**

You can submit messages that were incorrectly tagged as spam to Symantec Security Response. Symantec engineers will analyze the message and issue updates to the spam filtering rules as needed.

You can submit false positives to one of the following email addresses:

**North America**
Gfeedback@feedback-1.brightmail.com
Europe, Middle East, Africa
eurofeedback@feedback-23.brightmail.com

Japan, Asia, Pacific Rim
apacfeedback@feedback-22.brightmail.com

**Note:** These addresses are for false-positive messages only. You must send the message as an RFC-822 MIME-encoded attachment. You should include all header information, content, and attachments.
Introduction

About email filtering
The Spam Quarantine Report

This chapter includes the following topics:

■ About the Spam Quarantine Report
■ About the Spam Quarantine Summary

About the Spam Quarantine Report

The Spam Quarantine Report is an automatically generated report that is sent to your primary email address. It lists the email messages that have been filtered because of potential spam content. The Spam Quarantine Report includes email that was quarantined for your primary email address and any associated alias email addresses ("Maintaining your alias email addresses" on page 30).

If you or your administrator has configured your user account to receive text-based notifications of quarantined spam emails, you will receive a Spam Quarantine Summary instead of a Spam Quarantine report ("About the Spam Quarantine Summary" on page 14).

If your administrator has enabled this feature, the Spam Quarantine Report contains hyperlink commands that let you manage your quarantined email and change your configuration settings.

After you click a command, you are automatically logged into the Symantec Hosted Mail Security Console and the appropriate page is displayed. Depending on the selected command, you will see the results of the command action or you can continue with the desired action in the Symantec Hosted Mail Security Console.
In addition to the hyperlink commands, your Spam Quarantine Report contains the following information:

- All email addresses whose quarantined emails are included in the report
- Date, time, and time zone when an email was quarantined
- Sender email address of the quarantined email
- Subject line of the quarantined email
- Spam score of the quarantined email
  - A score of 90-99% indicates a medium likelihood that the email is spam.
  - A score of 99.1-100% indicates a high likelihood that the email is spam.
- File size, including all attachments, of the quarantined email

**Warning:** If you provide your Spam Quarantine Report to someone else (for example, by forwarding it in your email application), that person can log in to the Symantec Hosted Mail Security console as you using the links in the email, and has complete access to your configuration settings and your quarantined messages.

Your administrator may have designated that the commands in the Spam Quarantine Report expire after a set period of time. If you click a command that has expired, you will be prompted to log on to the console by using your user name and password.

The following list provides information about each command in the Spam Quarantine Report and the correlating page or option in the Symantec Hosted Mail Security Console.

The commands in Table 2-1 are available in the Spam Quarantine Report only if your administrator has configured the Spam Quarantine Reports to include them. Also, some commands may not be available in the console if your administrator has disabled those features in Symantec Hosted Mail Security.

<table>
<thead>
<tr>
<th>Action Description</th>
<th>Spam Quarantine Report</th>
<th>Symantec Hosted Mail Security Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage primary and alias email</td>
<td>Manage My Email Addresses</td>
<td>User Aliases page</td>
</tr>
<tr>
<td>addresses</td>
<td>command</td>
<td>(&quot;Maintaining your alias email</td>
</tr>
<tr>
<td></td>
<td></td>
<td>addresses&quot; on page 30)</td>
</tr>
</tbody>
</table>
### Table 2-1  Cross-reference of Features Between Spam Quarantine Report and Symantec Hosted Mail Security Console

<table>
<thead>
<tr>
<th>Action Description</th>
<th>Spam Quarantine Report</th>
<th>Symantec Hosted Mail Security Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>View emails quarantined on a specified date</td>
<td>Display a page to view quarantine for this day command</td>
<td>Message Quarantine page with a specific date selected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(&quot;Managing your personal Message Quarantine&quot; on page 19)</td>
</tr>
<tr>
<td>View email contents</td>
<td>Subject command in the desired email</td>
<td>Subject command on the Message Quarantine page</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(&quot;Reviewing a single quarantined email&quot; on page 20)</td>
</tr>
<tr>
<td>Release an email for delivery</td>
<td>Release command next to the desired email</td>
<td>Release button on the Safe Message View page</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(&quot;Reviewing a single quarantined email&quot; on page 20)</td>
</tr>
<tr>
<td>Add sender email address to allow list and release the</td>
<td>Always Allow command next to the desired email</td>
<td>Allow/Deny Sender Lists page</td>
</tr>
<tr>
<td>email for delivery</td>
<td></td>
<td>(&quot;Adding a single sender to an allow or deny list&quot; on page 23)</td>
</tr>
<tr>
<td>Add sender email address to deny list (if enabled) and</td>
<td>Deny command next to the desired email</td>
<td>Allow/Deny Sender Lists page</td>
</tr>
<tr>
<td>delete the email</td>
<td></td>
<td>(&quot;Adding a single sender to an allow or deny list&quot; on page 23)</td>
</tr>
<tr>
<td>Delete all the quarantined email</td>
<td>Delete All Messages command</td>
<td>Select All checkbox and delete button on the Message Quarantine page</td>
</tr>
<tr>
<td></td>
<td>Note: Only those messages listed in the current report will be deleted. If there are</td>
<td>(&quot;Deleting multiple emails&quot; on page 21)</td>
</tr>
<tr>
<td></td>
<td>more emails in your spam quarantine that are not listed, you must log into the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Symantec Hosted Mail Security Console to delete all the messages in your spam</td>
<td></td>
</tr>
<tr>
<td></td>
<td>quarantine area.</td>
<td></td>
</tr>
<tr>
<td>Set your preferences for Spam Quarantine Reports and</td>
<td>The click here command in the To change your spam report settings, click here at the</td>
<td>Preferences page</td>
</tr>
<tr>
<td>spam filtering.</td>
<td>bottom of the Spam Quarantine Report.</td>
<td>(&quot;The alias email address is deleted immediately.&quot; on page 35)</td>
</tr>
</tbody>
</table>
About the Spam Quarantine Summary

You will receive the Spam Quarantine Summary if you or your administrator has configured your user account to receive text-based notifications of quarantined spam emails instead of the Spam Quarantine Report. Usually, this option is designated if your email application does not support HTML content, which the Spam Quarantine Report contains.

The Spam Quarantine Summary indicates how many new emails have been quarantined as spam since the last Summary and the total number of quarantined spam emails in your spam quarantine.

You can click the hyperlink in the email to log into the Symantec Hosted Mail Security Console or you can copy the entire hyperlink into the Address field of your Web browser. Once you are logged into the Symantec Hosted Mail Security Console, the Message Quarantine page is displayed (see “Managing your personal Message Quarantine” on page 19 for more information).
Using the console

This chapter includes the following topics:
- Overview of the Symantec Hosted Mail Security Console
- Setting or changing your password
- Logging into the Symantec Hosted Mail Security Console
- Managing your personal Message Quarantine
- Maintaining Allow and Deny lists
- Configuring your preferences
- Maintaining your alias email addresses
Overview of the Symantec Hosted Mail Security Console

The Symantec Hosted Mail Security Console contains options for you to use to navigate through the available pages:

- **Quarantine** displays the Message Quarantine page, where you manage your quarantined email messages (potential spam).
- **Allow / Deny** displays the Allow/Deny Sender Lists page (“Maintaining Allow and Deny lists” on page 23) where you manage your personal allow and deny lists.
- **Setup** displays the Configuration page where you can change your password (“Logging into the Symantec Hosted Mail Security Console” on page 19), set your preferences (“The alias email address is deleted immediately.” on page 35) or maintain your alias email addresses (“Maintaining your alias email addresses” on page 30).
- **Logout** logs you out of the Symantec Hosted Mail Security Console.

Setting or changing your password

The first time you use the Symantec Hosted Mail Security Console, you must set a password that you will use thereafter to login. After you have logged into the Symantec Hosted Mail Security Console, you can change your password at any time.

Your password must be at least 6 characters long and cannot contain spaces. Passwords are case-sensitive. For security reasons, avoid using simple passwords that can easily be discovered.

If you do not have a password or have forgotten it, you can access the Console from your Spam Quarantine Report, if you have received one.

If you have forgotten your password and you have not received a Spam Quarantine Report, see “Requesting a password” on page 16.

Requesting a password

If you do not have a password or have forgotten it, you can request a new password. An email message will be sent to your email address that contains a hyperlink that lets you reset your password.

You can request a password through the Symantec Hosted Mail Security Console or through your Spam Quarantine Report.
To request a password using the console log on page

1. In your Web browser, go to the Symantec Hosted Mail Security portal at: https://hostedmailsecurity.symantec.com

2. On the Login page, click the hypertext link that is contained in the following line:
   If you can't remember your password or if you are having problems logging in, please click here.

3. Type your email address in the Email Address box and click Submit.
   After Symantec Hosted Mail Security validates the email address, you will receive an email message that contains a hyperlink that lets you reset your password. The hyperlink is active for only a limited time after the email is sent (typically, 60 minutes).

To request a password using your Spam Quarantine Report

1. At the bottom of your Spam Quarantine Report, click the hyperlink that is contained in the following line:
   To set a Hosted Mail Security Console password enabling you to login to your message quarantine, click here.
   Your default Web browser opens and you are automatically logged on to the Symantec Hosted Mail Security Console and the Configuration > Password Change page is displayed.

2. Click the here hyperlink that is contained in the following text:
   If you have not yet set a password or have forgotten your existing password, click here and an email will be sent to your mailbox allowing you to set a new password.
   After Symantec Hosted Mail Security validates the email address, you will receive an email message that contains a hyperlink that lets you reset your password. The hyperlink is active for only a limited time after the email is sent (typically, 60 minutes).

Resetting your password

Use this procedure to reset your password after you receive the email message from Symantec Hosted Mail Security that contains the instructions and hyperlink for resetting your password.

To reset your password

1. In the email message from Symantec Hosted Mail Security, click the hyperlink that is contained in the message to display the Configuration > Set Password page.
   The Set Password page is displayed.
2 In the **New Password** field, type the password you want to use. The typed text appears as dots for security reasons.

3 In the **Retype New Password** field, retype the password you want to use, exactly as you typed it in step 2.

4 Click **Continue**. If the password change was successful, a confirmation is displayed.

5 Click **OK** to continue. Your password is set.

### Changing your password

Perform this procedure to change your existing password.

**To change your password**

1 Do one of the following:
   - Click the **click here** command in the following text at the bottom of the Spam Quarantine Report that you received:
     
     To set a Symantec Hosted Mail Security Console password enabling you to login to your message quarantine, click [here](#).

     Your default Web browser opens and you are automatically logged on to the Symantec Hosted Mail Security Console and the Configuration > Password Change page is displayed.

     ■ If you already have a password, log into the Symantec Hosted Mail Security Console and click **Setup**. The Password Change page is displayed.

   - In the **Old Password** field, type your existing password. This step validates that you are authorized to change the password for the designated email address.

2 In the **New Password** field, type the new password you want to use. The typed text appears as dots for security reasons.

3 In the **Retype New Password** field, retype the password you want to use, exactly as you typed it in step 3.

4 Click **Continue**. Your password is set.
Logging into the Symantec Hosted Mail Security Console

You can log on to the Symantec Hosted Mail Security Console using any of the following methods:

- Click a command in your Spam Quarantine Report or Spam Summary Report.
  Your Spam Quarantine Report contains multiple commands that automatically log you on to the Symantec Hosted Mail Security Console.

- Log on directly to the Symantec Hosted Mail Security Console.
  Your email address and password must be registered in Symantec Hosted Mail Security to log on to the console directly. If you do not have a user account, contact your administrator.

If the Symantec Hosted Mail Security Console detects that no activity has taken place for a specific time interval (typically, 3 hours), it automatically logs you out.

To log on to the Symantec Hosted Mail Security Console

1. In your Web browser, go to the Symantec Hosted Mail Security portal at: https://hostedmailsecurity.symantec.com
2. On the Symantec Hosted Mail Security Console Login page, in the Email Address field, type the full email address of the primary or alias account that you want to use.
3. In the Password field, type your password.
   Passwords are case-sensitive.
4. If desired, choose an alternate language from the Language drop-down list.
   This preference will be saved for you the next time you log in.
5. Click Login.
   This opens the Symantec Hosted Mail Security Console and displays the Message Quarantine page.

Managing your personal Message Quarantine

The Message Quarantine contains email messages that were quarantined because of potential spam content as defined by the policies set by your administrator.
Managing your personal Message Quarantine

You can do the following from the Message Quarantine page:

- View the contents of quarantined email messages (See “Reviewing a single quarantined email” on page 20).
- Delete unwanted email messages (See “Deleting multiple emails” on page 21).
- Release email messages, which removes them from the quarantine and sends them to your primary email address (See “Releasing multiple emails” on page 21).
- Select the email addresses that you want to include in the report, if you have alias email addresses that are associated with your primary email address (See “Maintaining your alias email addresses” on page 30).
- Select specific sender (from) email addresses from which email will always be received or denied (See “Maintaining Allow and Deny lists” on page 23).

The Message Quarantine opens by default when you first log on to the console. You can sort the information in the Message Quarantine page by column headings. You can view all of the messages that are in your quarantine or filter by dates.

Selecting which email addresses to include

You can select which of your associated email addresses to view on the Message Quarantine page. For example, you can view all your email addresses, only your primary email address, or any of your alias email addresses. If you have no alias email addresses associated with this primary email address, this option is not available. See “Maintaining your alias email addresses” on page 30 for more information about primary and alias email addresses.

To select which email addresses to include
1. From the Symantec Hosted Mail Security Console, click Quarantine.
2. On the Message Quarantine page, in the Sent To list, select the email address option that you want to use.

Reviewing a single quarantined email

You can view the contents of a single email and then delete or release it. The email is opened on a “safe” page in the Symantec Hosted Mail Security Console for your review.
To review a single quarantined email

1. From the Symantec Hosted Mail Security Console, click Quarantine.
2. On the Message Quarantine page, under the Subject column, click the link to the message that you want to view.
   The email contents open on a Safe Message View page.
3. Do one of the following:
   - To add the “from” email address to your Allow list, click **Always Allow** (See “Maintaining Allow and Deny lists” on page 23). The email address is added to the Allow list on the Allow/Deny Sender Lists page.
   - To add the “from” email address to your Deny list, click **Always Deny** (See “Maintaining Allow and Deny lists” on page 23). This feature is optional and may be unavailable if your administrator disabled it. The email address is added to the Deny list on the Allow/Deny Sender Lists page.
   - To accept the email and have it forwarded to your primary email address, click **Release** on the bottom of the Safe Message View page. If the email was originally sent to an alias email address, the email is released to the primary email address.
   - To delete the email, click **Delete**.
4. To return to the Message Quarantine page, click **Quarantine Index**.

Releasing multiple emails

You can release one or more emails from the Message Quarantine at the same time. Released emails are sent to your primary email address.

To release multiple emails

1. On the Message Quarantine page, select the checkbox in front of each email that you want to release, or check the **All** checkbox to select all of the messages in the list.
2. Click **Release** to release the selected messages immediately to your primary email address.
   If the email message was originally sent to an alias email address, the email is released to the primary email address.

Deleting multiple emails

You can delete one or more email messages at the same time.
Managing your personal Message Quarantine

To delete multiple email messages

1. From the Symantec Hosted Mail Security Console, click **Quarantine**.
2. On the Message Quarantine page, select the checkbox in front of each email that you want to delete, or check the **All** checkbox to select all of the messages in the list.
3. Click **Delete** to delete the selected messages immediately.

Adding senders to an Allow list from the Message Quarantine

You can add the senders of one or more messages in your Message Quarantine to your Allow list. Thereafter, all messages that are received from these email addresses will be accepted without filtering for spam content. Messages are always scanned for viruses.

To add multiple senders to an Allow list

1. From the Symantec Hosted Mail Security Console, click **Quarantine**.
2. On the Message Quarantine page, select the checkbox in front of each email that you want to delete, or check the **All** checkbox to select all of the messages in the list.
3. Click **Always Allow** to add the email addresses to your Allow list.

Adding senders to a Deny list from the Message Quarantine

You can add the senders of one or more email messages in your Message Quarantine to your Deny list. Thereafter, all emails from these email addresses always be denied delivery.

To add multiple senders to a Deny list

1. From the Symantec Hosted Mail Security Console, click **Quarantine**.
2. On the Message Quarantine page, select the checkbox in front of each email that you want to delete, or check the **All** checkbox to select all of the messages in the list.
3. Click **Always Deny** to add the email addresses to your Deny list.
   This feature is optional and may be unavailable if your administrator disabled it.
Maintaining Allow and Deny lists

You can define lists of senders whose email addresses either will always be accepted without spam filtering (Allow list) or will never be accepted for delivery (Deny list). You can add senders to these lists from the Message Quarantine page or from the Allow/Deny Sender Lists page.

Note: A common technique of spammers is to change their sender email address often. A deny list may not prevent spam messages from these senders. The deny list primarily is used to block email messages from unwanted senders that you know or that have stable email addresses.

There are two basic definitions of spam that may help you determine whether a sender address should be added to your Deny list:

- The first type of spam includes unwanted message that are received from recognized senders.
  For example, a salesperson for a company may be sending you unwanted messages. In this scenario, it is unlikely that the sender address will be changed often, so this type of address would be a good candidate to be added to Deny list.

- The second type of spam includes unwanted email messages that contain malicious, questionable, or offensive content. These types of messages are usually sent from spammers who deliberately attempt to bypass blacklisting and content filtering rules. For example, you may receive email messages from a sender with a fraudulent money-making offer or messages that contain offensive sexual content. In this scenario, the spammers often change their email addresses and use techniques to evade blacklist filtering. This type of address is not a good candidate to be added to the Deny list because it is effective for only a brief time.

Adding a single sender to an allow or deny list

You can add a sender email address or domain to the designated list. For example, you can do any of the following:

- Designate a single email address (for example, “person@abc.com”) to force the emails received from just that address to be always or never delivered

- Designate an entire domain (for example, “abc.com”) to force the emails received from all addresses from that domain to be always or never delivered.
Maintaining Allow and Deny lists

- Use wildcards to enter a range of email addresses (for example, j*@abc.com) to force the emails received from all addresses starting with “j” from that domain to be always or never delivered.

The same address cannot be added multiple times in the same list or added to both the Allow and Deny lists. The Allow list overrides the Deny list. For example, if you designate a range of email addresses (for example, by designating an entire domain) in the Deny list, but then designate a single email address from that domain in the Allow list, the email from that single address will be always accepted while the email from any other address in the domain in the Deny list will be always denied.

Note: Your administrator can also define Allow and Deny lists. In this case, the settings made by the Administrator are applied before your settings.

To add a single sender to an allow or deny sender list
1. From the Symantec Hosted Mail Security Console, click Allow/Deny.
2. On the Allow/Deny Sender Lists page, in the appropriate Add Entry box, type the sender address that you want to add to the list.
3. Click Add.
   The email address appears in the list box.

Adding multiple senders to an Allow or Deny list

You can add a predefined list of email addresses or domain names to your Allow Sender list or your Deny Sender list. The predefined list must be a text file in the following format:

- One entry per line (domain name or email address)
- File must be available for your browser to access

Each entry in the list can include any of the following:

- A single email address (for example, “person@abc.com”) to force the emails received from just that address to be always or never delivered
- An entire domain (for example, “abc.com”) to force the emails received from all addresses from that domain to be always or never delivered
- Wildcards to enter a range of email address (for example, j*@abc.com) to force the emails received from all addresses starting with “j” from that domain to be always or never delivered.
Using the console

Maintaining Allow and Deny lists

Note: The same address cannot be added multiple times in the same list or added to both the Allow and Deny lists. Any duplicate or invalid email address or domain names are discarded automatically.

The Allow list overrides the Deny list. For example, if you designate a range of email addresses (for example, by designating an entire domain) in the Deny list, but then designate a single email address from that domain in the Allow list, the email from that single address will be always accepted while the email from any other address in the domain in the Deny list will be always denied.

To add multiple senders to an Allow or Deny list

1. From the Symantec Hosted Mail Security Console, click **Allow/Deny**.
2. On the Allow/Deny Sender Lists page, in the **Upload Allow List** or **Upload Deny List** field, type the full path and file name of the file that contains the list of email addresses that you want to add.
   Optionally, you can browse to the location of the file.
3. Click the appropriate **Upload File** button.
   The addresses from the file appear in the appropriate list.

Removing senders from an Allow or Deny list.

You can remove sender addresses from your Allow or Deny list.

To remove senders from an Allow or Deny List

1. On the Symantec Hosted Mail Security Console, click **Allow/Deny**.
2. On the Allow/Deny Sender Lists page, click to select the sender address in the appropriate list box.
3. Click **Remove** next to the list box where the sender addresses are selected.

Saving an Allow or Deny list to a file

You can save the contents of your Allow or Deny list to a file.

To save an Allow or Deny list to a file

1. On the Symantec Hosted Mail Security Console, click **Allow/Deny**.
2. On the Allow/Deny Sender Lists page, click **Download List** in the appropriate area.
3. Click **Save** to save the list to a file.
4 Type the file name that you want to use and the location in which you want to save the file, and then click Save.

Configuring your preferences

You specify settings that control your Spam Quarantine Reports and whether your email is filtered for spam.

Note: This page is only available if your Administrator has enabled spam filtering for your domain or has not disabled your ability to change these settings.

You can configure the following preferences:

- Select whether your email is filtered for spam. This feature is optional and may be unavailable if your Symantec Hosted Mail Security Administrator disabled it.
- Select what action will be taken if an email is likely spam. This feature is optional and may be unavailable if your Symantec Hosted Mail Security Administrator disabled it.
- Select how often you receive Spam Quarantine Reports. This feature is optional and may be unavailable if your Symantec Hosted Mail Security Administrator disabled it.
- Select which emails to include in your Spam Quarantine Report. This feature is optional and may be unavailable if your Symantec Hosted Mail Security Administrator disabled it.
- Select the time zone used to process your emails and Spam Quarantine Reports. This feature is optional and may be unavailable if your Symantec Hosted Mail Security Administrator disabled it.
- Select what language or languages in which you wish to receive email. This feature is set to All Languages by default.

To open the Preferences page

- Do one of the following:
  - On the Message Quarantine page, click the click here link at the bottom of the page.
  - On the Symantec Hosted Mail Security Console, click Setup.
Turning spam filtering on or off

You can select whether your email messages will be filtered for spam content. This feature is optional and may be unavailable if your administrator disabled it.

**Note:** This feature affects all of your associated email addresses, including your primary address and all alias email addresses.

1. On the Configuration > Preferences page, click to check or uncheck the **Do not filter my messages** checkbox.
2. Click the **Update** button below the checkbox description.

If you turn off spam filtering, the following occurs:
- All messages in your spam quarantine are released to your primary email address.
- The **Please email me a quarantine report every** field is set to Never and becomes unavailable.
- Your email is not filtered for spam thereafter.

If you activate spam filtering, the following occurs:
- The **Please email me a quarantine report every** field becomes available. To receive Spam Quarantine Reports, you must change this field to a value other than Never.
- Your email is filtered for spam thereafter.

Selecting spam email actions

You can designate what action will be taken if an email is determined to be likely spam. As the Symantec Hosted Mail Security analyzes your email, it assigns a likelihood to each email that it is spam. If an email is determined to have a medium or high likelihood of being spam, the designated action is performed on the email. You can choose to use the default actions defined by your Administrator or you can choose different actions.

The following actions are available:
- Quarantine the message: The email is added to your Spam Quarantined Messages area and is not sent to you. The email is reported in your Spam Quarantine Report.
- Prepend “[SPAM]” to message subject: The subject line of the email has the phrase “[SPAM]” added to the beginning of the subject text and the email is sent to you.


- Deny Delivery: The email is blocked automatically. Depending on the sending system’s configuration, the email sender may or may not be notified.

- Do Nothing: The email is forwarded to you with no processing applied.

This feature is optional and may be unavailable if your administrator disabled it. This feature is unavailable if you have turned off spam filtering (see “Turning spam filtering on or off” on page 27).

To select spam email actions

1. On the Setup > Configuration > Preferences page, click to check or uncheck the Use Group Actions checkbox.
   - If you checked Use Group Actions, go to step 2.
   - If you unchecked Use Group Actions, select the email action to use if your email is likely spam.
     Select the desired action for medium likelihood spam in the Medium Spam Action drop-down list.
     Select the desired action for high likelihood spam in the High Spam Action drop-down list.

2. Click Update below the Preferences area.

Selecting Spam Quarantine Report frequency

You can select how often you want to receive your Spam Quarantine Report. This feature is optional and may be unavailable if your administrator disabled it.

To select spam quarantine report frequency

1. On the Setup > Configuration > Preferences page, select the desired frequency in the Please email me a quarantine report every field:
   - Default: The frequency is set to the default configured by your Symantec Hosted Mail Security Administrator.
   - Every Day: The Spam Quarantine Reports are sent daily.
   - Every Weekday: The Spam Quarantine Reports are sent daily from Monday through Friday.
   - Every Monday: The Spam Quarantine Reports are sent each Monday.
   - Monday & Friday: The Spam Quarantine Reports are sent each Monday and Friday.
   - Monday, Wednesday, & Friday: The Spam Quarantine Reports are sent each Monday, Wednesday, and Friday.

2. Click Update below the Preferences area.
Selecting Spam Quarantine Report content

You can select what content you want included in your Spam Quarantine Report. This feature is optional and may be unavailable if your Administrator disabled it.

To select Spam Quarantine Report content
1. On the Setup > Configuration > Preferences page, select the desired content in the Include the following items in my report field:
   - Default: The content will be set to the default configured by your administrator.
   - All Quarantined Messages: All your quarantined emails will be listed.
   - New Items Since Last Report: Only those quarantined emails that were received since your previous Spam Quarantine Report will be listed.
   - Text-only Summary: A text message will be sent to your primary email address notifying you that you have emails in your spam quarantine area, with a link that will automatically log you into the Message Quarantine when clicked (see “About the Spam Quarantine Summary” on page 14).
2. Click Update.

Setting the time zone for your email processing

You can specify the time zone that will be used to designate your local time zone used when you log on to the Symantec Hosted Mail Security Console. The time and date of your Spam Quarantine Reports and the processed emails will be controlled by the time zone designated by the data center where the Symantec Hosted Mail Security is running.

If the time zone that you designate in this procedure differs from the data center, you may have to select a date different from your current local date in the Symantec Hosted Mail Security Console to view the data. For example, if your local time zone is 7 hours behind of the time zone of the data center, you may have to select the next day (“tomorrow”) in the calendar to view additional emails that may be in your Message Quarantine.

Alternatively, you can select to view all the emails and thus see all quarantined emails in the Message Quarantine.

To set the time zone for your email processing
1. On the Setup > Configuration > Preferences page, select the desired time zone in the Time Zone drop-down list.
Maintaining your alias email addresses

You must have a primary email address defined in Symantec Hosted Mail Security to log on to the Symantec Hosted Mail Security Console, to have email filtered, and to receive a Spam Quarantine Report. Your primary email address may have been defined by your administrator or Symantec Hosted Mail Security may have defined one for you automatically when it received email messages for your address.

You may have multiple primary email addresses, depending on whether you have been using multiple email addresses in the Symantec Hosted Mail Security. In this case, you would have multiple quarantine areas that you must log on to and manage, and you would receive multiple Spam Quarantine Reports (one for each primary email address).

Instead of having multiple primary email addresses, you can associate multiple email addresses to one primary email address. The associated email addresses are called alias email addresses. The maximum allowed number of alias email addresses is configured by your administrator. Each email address, primary and alias, must be unique within each domain. Each email address must be a valid address and configured on the email server at your company site.
Unless an email is quarantined, each email is sent to its designated recipient email address (that is, an email with a recipient address that is an alias email address is sent to that address, not to the primary email address).

If your administrator has defined alias domain names for your domain, you may see additional email addresses for those alias domain names in your email address list. An alias domain name provides the same type of email consolidation as an alias email address. When an alias domain name was defined for your domain, Symantec Hosted Mail Security automatically created the appropriate alias email addresses based on your primary email address in the alias domain. These addresses are listed for your information and are automatically aliased to your primary email address. You cannot set one of these automatically aliased email addresses to be your primary email address.

By using an alias email address, you would have one quarantine area to manage for each set of associated email addresses. You would receive one Spam Quarantine Report that includes the information for each primary address and all its associated alias email addresses. The Spam Quarantine Report is sent to the primary email address.

All messages that are released from the quarantine area are sent to the primary email address.

All the associated email addresses, primary and aliases, are controlled by the configuration settings for the primary email address.

**When you add an alias email address**

If you add an alias email address on the User Aliases page in the Symantec Hosted Mail Security Console, the following occurs:

- An email is sent to the added alias email address. The email contains a hyperlink command that the recipient must click to authorize the use of the alias email address.

- Once the command is clicked, the alias email address is authorized and associated with the primary email address. If the alias email address had previously been a primary email address, its user configurations are discarded, depending on the requirements specified in “‘Converting a primary email address to an alias address’” on page 32.

- Thereafter, the quarantine information for the alias address will be combined with the quarantine for the primary email address and it will be controlled by the user configuration for the primary email address.
If you add an alias email address using the Manage My Email Addresses command in the Spam Quarantine Report, the following occurs:

- If the email address that received the Spam Quarantine Report already has alias email addresses associated to it, the Symantec Hosted Mail Security Console is opened to the Setup> Configuration > Aliases page in your local browser. You can then perform your alias email address management.

- If the email address that received the Spam Quarantine Report does not already have alias email addresses associated to it, the Symantec Hosted Mail Security Console is opened to a page that prompts you for your primary email address (the email address to which you want to associate alias email addresses).
  - An email is sent to that primary address. The email contains a hyperlink command that the recipient (most likely you) must click to confirm that you are authorized to change its use.
  - Once the recipient clicks the authorization command in the email in the local email application, the Symantec Hosted Mail Security Console is opened to the Setup > Configuration > Aliases page.
  - The recipient can then perform the alias email address management.

Converting a primary email address to an alias address

You can convert a primary email address into an alias email address by doing one of the following:

- Within a set of a primary email addresses and its associated alias email addresses, you can switch between the addresses to designate which is the primary email address.

- You can add an existing primary email address to be an alias to another primary email address. In this case, the user configuration (for example, allow and deny lists) for the newly aliased email address is deleted from the system after the aliasing is completed.

You cannot add a primary email address that already has associated alias email addresses to be an alias email address to another primary email address (for example, nested alias email address). In this case, you must first delete all the alias email addresses associated to the primary email address being aliased.

Deleting associated email addresses

You can delete alias email addresses, but you cannot delete a primary email address. Only the Symantec Hosted Mail Security Administrator can delete primary email addresses.
Maintaining your alias email addresses

If the primary address email is associated to alias email addresses, you can designate that one of the alias email addresses be set to be the primary email address. This causes the old primary email address to become an alias email address to the new primary email address. Then you can delete the old primary email address.

If you delete an alias email address, its association with the primary email address is removed and it will no longer be controlled by the primary email address’ user configuration (for example, allow and deny lists). If you continue to receive email to the deleted email address, Symantec Hosted Mail Security may automatically recreate the email address as a primary email address for you with default user configurations, depending on system configurations.

Accessing the User Aliases settings

The Setup > Configuration > Aliases page is the location where you manage your alias email addresses. You can do the following:

- Select which of your associated email addresses is your primary email address
- Delete an alias email address
- Add a new alias email address to your primary email address

To access the User Aliases page

- Do one of the following:
  - Log into the Symantec Hosted Mail Security Console and click Setup. On the Configuration page, click Aliases.
  - In the Spam Quarantine Report, click Manage My Email Addresses.

If you currently have alias email addresses defined, the Setup Configuration > Aliases page is displayed.

If you do not have alias email addresses defined, you are prompted for your primary email address.

Type your email address and click Submit.

An authorization email is sent automatically to the entered email address requesting authorization for the change. After you receive the email message, click the hyperlink command that is contained in the message. This sends an authorization to the hosted mail security service, which then opens the Console in your default Web browser.

Selecting which email address is primary

If you already have alias email addresses associated with your primary email address, this procedure lets you select which of the listed addresses is your...
primary email address. The user configuration settings (for example, allow and
deny lists) are transferred to the selected primary email address. The Spam
Quarantine Report and any emails released from quarantine will be sent to the
primary email address.

The primary email address always is first in the list of email addresses and has
the text Primary in the Type column. The alias email addresses have the text
User Alias in the Type column and the command [Delete] after them.

If your Administrator has defined alias domain names for your domain, an alias
email address was automatically created for your primary email address using
the alias domain name. This type of alias email address is shown with the text
Domain Alias in the Type column and is not available for selection as a primary
email address.

To select which email address is primary
- On the Setup > Configuration > Aliases page, select the radio button in front
  of the email address that you want to select as your primary email address.
The selected email address is set immediately to be your primary email
address.

Adding an alias email address

You can add an alias email address to the shown primary email address. If the
added alias email address had been used as a primary email address, its user
configuration will be deleted after the addition is authorized, and it will be
controlled by the user configuration of the primary email address.
Authorization emails will be sent to the added alias email addresses to confirm
that you have the authority to change their use.

To add an alias email address
1. On the Setup > Configuration > Aliases page, in the Add an Alias Email
   Address for {primary address} box, type the email address to be added as an
   alias email address, where {primary address} is the current primary email
   address.
   If necessary, select a domain in the Domain drop-down list to the right of
   the @ character.
   This list appears only if your domain has alias domain names associated
   with it.
2. Click Add.
   An authorization email is sent automatically to the added email address
   requesting authorization for the change.
3 The recipient of the email (most likely you) must click the hyperlink command in the authorization email to continue the alias addition.

4 Immediately after Symantec Hosted Mail Security receives the authorization, the email address is added as an alias email address to the listed primary email address.

Deleting an alias email address

You can delete an alias email address, which removes its association with the primary email address. If you continue to receive email to the deleted address, Symantec Hosted Mail Security may recreate the email address as a primary email address with default user configurations, depending on system configurations. You cannot delete a primary email address (see “Deleting associated email addresses” on page 32).

To delete an alias email address

1 If the email address that you want to delete is the primary email address, you must convert the primary address to an alias email address.

2 On the Setup > Configuration > Aliases page, click Delete next to the alias email address that you want to delete. The alias email address is deleted immediately.
Maintaining your alias email addresses