Email Defense Portal & Spam Quarantine Report
End User Guide

Release Date: March 29, 2004
# Table of Contents

1. **Introduction** ........................................................................................................ 1-1
   1.1. Wrong Email Got Past Filter ....................................................................... 1-1

2. **Spam Quarantine Report** .................................................................................. 2-1

3. **Email Defense Portal** ........................................................................................ 3-1
   3.1. Overview of the Email Defense Portal Window ........................................ 3-1
   3.2. Window Navigation ..................................................................................... 3-2
   3.3. Setting/Changing Your Password ............................................................... 3-3
      3.3.1. Forgot Your Password? ..................................................................... 3-4
   3.4. Logging into the Email Defense Portal ........................................................ 3-5
   3.5. Managing Your Personal Message Quarantine .......................................... 3-7
      3.5.1. Select Which Email Address to List ................................................... 3-8
      3.5.2. Review Single Quarantined Email ..................................................... 3-9
      3.5.3. Release Multiple Emails .................................................................. 3-10
      3.5.4. Delete Multiple Emails ..................................................................... 3-10
      3.5.5. Add Multiple Senders to Allow List .................................................. 3-10
      3.5.6. Add Multiple Senders to Deny List ................................................... 3-11
      3.5.7. Select Spam Quarantine Report Frequency .................................... 3-11
      3.5.8. Select Spam Quarantine Report Content ........................................ 3-11
      3.5.9. Turn Off/On Spam Filtering ............................................................. 3-12
   3.6. Maintaining Your Allow/Deny Lists ........................................................... 3-12
      3.6.1. Add Single Sender to Allow List or Deny List .................................. 3-14
      3.6.2. Add Multiple Senders to Allow List or Deny List .............................. 3-15
      3.6.3. Remove Senders from Allow List or Deny List................................... 3-16
   3.7. Maintaining Your Alias Email Addresses .................................................. 3-16
      3.7.1. Select Which Email Address is Primary ........................................... 3-20
      3.7.2. Add an Alias Email Address ............................................................ 3-21
      3.7.3. Delete an Alias Email Address ......................................................... 3-22
List of Figures

Figure 1: Spam Quarantine Report................................................................. 2-1
Figure 2: Email Defense Portal window overview............................................ 3-1
Figure 3: Configuration - Password Change window........................................ 3-3
Figure 4: Email Defense Portal - Login window.............................................. 3-4
Figure 5: Lost password request window......................................................... 3-5
Figure 6: Email Defense Portal - Login window.............................................. 3-6
Figure 7: Message Quarantine window............................................................. 3-6
Figure 8: Unsuccessful login window............................................................... 3-7
Figure 9: Message Quarantine window............................................................. 3-8
Figure 10: Safe Message View window............................................................ 3-9
Figure 11: Allow/Deny Sender Lists window.................................................... 3-14
Figure 12: Configuration - Aliases window..................................................... 3-20

List of Tables

Table 1: Cross-reference of Features Between Spam Quarantine Report and Email Defense Portal ................................................................. 2-2
Table 2: Tab Options......................................................................................... 3-2
1. Introduction

The Email Defense Service enables you to manage your personal message quarantine system. The Email Defense Service quarantines emails that are suspected to be spam in a safe location. You will receive Spam Quarantine Reports or a text-based via email on a regular basis notifying you that you have quarantined email (see “Spam Quarantine Report” on page 2-1 for more information). You then log into the Email Defense Portal and manage your quarantined email.

In the Email Defense Portal, you can perform any of the following (depending on your system's configuration):

- Create or change your password for the Email Defense Portal (see page 3-3)
- Log into the Email Defense Portal (see page 3-5)
- Manage the emails in your quarantine area (see page 3-7)
- Manage your personal “Allow/Deny” lists (see page 3-12)
- Configure additional email addresses to be included in your Spam Quarantine Report (see page 3-16)

From the Spam Quarantine Report, you can perform most of the same actions that are available in the Email Defense Portal.

**Important Note:** The Email Defense Service 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 Email Defense Service administrator.

1.1. Wrong Email Got Past Filter

What do you do if spam email, virus email, etc., was delivered anyway?

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

1. Check that the email addresses were not added to an **Allow** list by either you or your Email Defense Service administrator (see “Maintaining Your Allow/Deny Lists” on page 3-12 for more information).

2. Confirm with your Email Defense Service administrator that the policy settings in the Email Defense Service have not been changed to allow these emails to bypass filtering.
3. If you have determined that your system was not configured to let these emails bypass filtering, forward the email with all header information, content, and attachments to spam@emaildefenseservice.com.

MX Logic personnel will analyze the email information to refine the filtering engines for subsequent release, and if necessary, post any urgent updates to virus scanners, etc., to support filtering these emails properly.
2. Spam Quarantine Report

The Spam Quarantine Report is an automatically generated report sent to your primary email address that lists the emails that have been filtered because of potential spam content. The Spam Quarantine Report includes email that was quarantined for your primary email address and all its associated alias email addresses (see “Maintaining Your Alias Email Addresses” on page 3-16 for more information about primary and alias email addresses).

Figure 1: Spam Quarantine Report

The Spam Quarantine Report contains command links that allow you to manage your quarantined email and change your configurations. After you select an action command, you are automatically logged into the Email Defense Portal and the appropriate window opens. Depending on the selected action, you will see the results of the action command or you can continue with the desired action in the Email Defense Portal.

Important Note: If you provide your Spam Quarantine Report to someone else (for example, by forwarding it in your email application), that person would have complete access to the Email Defense Portal with your login information and thus could change your configurations, manage your quarantined email, etc. Be very careful to control access to your Spam Quarantine Report.

The following list provides a cross-reference of each command in the Spam Quarantine Report and the correlating window/field in the Email Defense Portal.
<table>
<thead>
<tr>
<th>Action Description</th>
<th>Spam Quarantine Report</th>
<th>Email Defense Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage primary and alias email addresses</td>
<td>Manage My Email Addresses command</td>
<td>Configuration – User Alias window (see “Maintaining Your Alias Email Addresses” on page 3-16)</td>
</tr>
<tr>
<td>View email contents</td>
<td>Subject command</td>
<td>Subject command in the Message Quarantine window (see “Review Single Quarantined Email” on page 3-9)</td>
</tr>
<tr>
<td>Release an email for delivery</td>
<td>Release command next to the desired email</td>
<td>Release button in the Message Quarantine – Safe Message View window (see “Review Single Quarantined Email” on page 3-9)</td>
</tr>
<tr>
<td>Add sender email address to deny list (if enabled) or allow list</td>
<td>Allow command or Deny command</td>
<td>Allow/Deny Sender Lists window (see “Add Single Sender to Allow List or Deny List” on page 3-14)</td>
</tr>
<tr>
<td>Delete all the quarantined email</td>
<td>Delete All Messages command</td>
<td>Select All checkbox and delete button in the Message Quarantine window (see “Delete Multiple Emails” on page 3-10)</td>
</tr>
<tr>
<td>Control report frequency (if this feature is enabled)</td>
<td>Please deliver this report every commands</td>
<td>Please email me a quarantine report every field in the Message Quarantine window (see “Select Spam Quarantine Report Frequency” on page 3-11)</td>
</tr>
</tbody>
</table>

Note: if the Spam Quarantine Report contains only messages received since the last report, only those messages listed in the current report will be deleted. In this case, you must log into the Email Defense Portal to delete all the messages in your spam quarantine area.
<table>
<thead>
<tr>
<th>Action Description</th>
<th>Spam Quarantine Report</th>
<th>Email Defense Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control report content (if this feature is enabled)</td>
<td>Include the following items in the report commands</td>
<td>Include the following items in the report field in the <strong>Message Quarantine</strong> window (see “Select Spam Quarantine Report Content” on page 3-11)</td>
</tr>
<tr>
<td>Control whether your email is filtered for spam (if this feature is enabled)</td>
<td>If you prefer to not have your email filtered for spam, <a href="#">click here</a>.</td>
<td>I prefer to not have my messages filtered for spam checkbox in the <strong>Message Quarantine</strong> window (see “Turn Off/On Spam Filtering” on page 3-12)</td>
</tr>
<tr>
<td>Set your Email Defense Portal password (if this feature is enabled)</td>
<td>To set a Email Defense Portal password enabling you to login to your message quarantine, <a href="#">click here</a>.</td>
<td>Configuration – Password Change window (see “Setting/Changing Your Password” on page 3-3)</td>
</tr>
</tbody>
</table>
3. Email Defense Portal

3.1. Overview of the Email Defense Portal Window

Figure 2 shows the GUI elements of the Email Defense Portal. Note that the actual window elements may differ depending on which window is open and what features are enabled.

Figure 2: Email Defense Portal window overview

Tab Options: Click the appropriate tab option to access the desired menu options and/or windows. See “Window Navigation” on page 3-2 for information about each tab option.

Window: The contents of each window change to reflect the menu options, commands, and relevant information for the selected menu option and/or actions performed in this area.

Menu Options: Click the menu option to access additional windows. When the window first opens, the left-most menu option is selected automatically. See the description for each window to see which menu options are available.
Field  A field allows you to select, type, or check information to perform functions. For example, you can type in text, click to highlight a choice in a drop-down list, or check or uncheck an option.

Button  A button has a border and performs a function immediately after being clicked. For example, clicking the **Update** button applies all changes in certain windows.

Commands  Depending on the window, hyperlink commands may be available. A command performs a function, such as displaying more information or opening a new page. Click the command to perform the action.

Help Information  Additional information about the features in the window will appear at the bottom of the window in a bordered box. The information will change depending on which window is open. If available, you can click the **[what’s this?]** command to display information about a specific feature.

### 3.2. Window Navigation

The Email Defense Portal contains a list of tab options that enables you to navigate through the available windows.

<table>
<thead>
<tr>
<th>![Quarantine]</th>
<th>![Allow / Deny]</th>
<th>![Setup]</th>
<th>![Logout]</th>
</tr>
</thead>
</table>

Table 2 describes the functions of the tab options.

**Table 2: Tab Options**

- The **Quarantine** tab option opens the **Message Quarantine** window (see page 3-7) where you manage your quarantined email messages (potential spam) and configure features in your Spam Quarantine Reports.

- The **Allow / Deny** tab option opens the **Allow/Deny Sender Lists** window (see page 3-12) where you manage your personal allow and deny lists.

- The **Setup** tab option opens the **Configuration** window where you can change your password (see page 3-3) or maintain your alias email addresses (see page 3-16).

- The **Logout** button exits you from the **Email Defense Portal**.
3.3. Setting/Changing Your Password

The first time you try to access the Email Defense Portal, you must define a password that you will use thereafter to login. After you have logged into the Email Defense Portal, you can change your password at any time.

This feature is optional and may be unavailable if your Email Defense Service administrator disabled it.

Your password must be at least 6 characters and/or digits long. You cannot use spaces. Passwords are case-sensitive (for example, “Password”, “password”, and “PASSword” would be different passwords).

Make sure you can remember your password, but do not use obvious passwords (for example, “password”, your name, or a family member’s name). Keep your password safe and private.

If you have forgotten your password, see “Forgot Your Password?” on page 3-4.

Procedure

Open the Configuration - Password Change Window

1. Do one of the following:
   a. Navigate to the bottom of the Spam Quarantine Report that you received until you see the following text:
      To set a Email Defense Portal password enabling you to login to your message quarantine, click here.
      1) Click the click here command.
      The Email Defense Portal initiates, you are automatically logged in, and the Configuration – Password Change window appears.
   b. If you already have a password, log into the Email Defense Portal (see “Logging into the ” on page 3-5).
      1) In the Email Defense Portal, click the Setup tab option.
      The Configuration – Password Change window appears.

---

Figure 3: Configuration - Password Change window
Change Password

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 the **Continue** button.

Your password is set. Use this password to log into the Email Defense Portal in the future.

### 3.3.1. Forgot Your Password?

If you forgot your password, you can request that an email be sent to your email address with a command link allowing you to reset your password.

**Procedure**

1. In your Web browser, enter the URL for your Email Defense Portal in the **Address** field:

   The **Email Defense Portal - Login** window appears.

   ![MX Control Console](image)

   **Figure 4: Email Defense Portal - Login window**

2. Optionally, click a command in the **News** area to view the contents of the selected item.

   The list of items may differ depending on your system's configuration.

   a. When finished, click the Back button in your Web browser to return to the **Email Defense Portal - Login** window.

3. In the **Email Defense Portal - Login** window, find the following text:

   **If you can't remember your password or if you are having problems logging in, please click here.**

   a. Click the **click here** command.

   The following window appears.
4. Type your email address in the **Email Address** field and click the **submit** button.
   
   The Email Defense Service validates the entered email address and sends an email to that address with a command link that will allow you to reset your password.

5. In your local email application, click the command link in the email.
   
   The Email Defense Portal initiates in your Web browser and you are automatically logged in.

6. Change your password (see “Setting/Changing Your Password” on page 3-3).

3.4. Logging into the Email Defense Portal

You must have an email address and password registered with the Email Defense Service to log into the Email Defense Portal. See “Setting/Changing Your Password” on page 3-3 for more information about your password configuration.

This feature is optional and may be unavailable if your Email Defense Service administrator disabled it. If this feature is unavailable, you must use your Spam Quarantine Report to access the Email Defense Portal (see "Spam Quarantine Report" on page 2-1 for more information).

**Note**: Your Spam Quarantine Report contains multiple commands that automatically log you into the Email Defense Portal, bypassing the Email Defense Portal – Login window. See “Table 1: Cross-reference of Features Between Spam Quarantine Report and Email Defense Portal” on page 2-2 for a list of these commands.

If the Email Defense Portal detects that no activity has taken place for 30 minutes, it will automatically log you out.

**Procedure**

1. In your Web browser, enter the URL ([http://portal1.emaildefenseservice.com](http://portal1.emaildefenseservice.com)) for your Email Defense Portal in the **Address** field:
   
   The Email Defense Portal - Login window appears.
Figure 6: Email Defense Portal - Login window

2. Optionally, click a command in the **News** area to view the contents of the selected item.
   
   The list of items may differ depending on your system’s configuration.
   
   a. When finished, click the Back button in your Web browser to return to the **Email Defense Portal – Login** window.

3. Enter your email address and password in the appropriate fields.
   
   The fields are case-sensitive. Your email address should be all lower-case.

4. Click the **login** button.
   
   If your login is successful, the Email Defense Portal initializes, displaying the **Message Quarantine** window.

Figure 7: Message Quarantine window

You are now logged into the Email Defense Portal.
Procedure if Login Is Unsuccessful

1. If your login is unsuccessful, an error message displays in red on the login window.

![Unsuccessful login window](image)

Figure 8: Unsuccessful login window

2. Retry logging in. If you are unsuccessful again, see “Forgot Your Password?” on page 3-4 for the procedure to request assistance with your login information or contact your Email Defense Service administrator.

3.5. Managing Your Personal Message Quarantine

The Message Quarantine window is the location where you manage your emails that were quarantined because of potential spam content as defined by the policies set by your Email Defense Service administrator. In the Message Quarantine window, you can do the following:

- View the contents of quarantined emails (see page 3-9)
- Delete unwanted emails (see pages 3-9 and 3-10).
- Release desired emails, which takes them out of quarantine and sends them to your primary email address (see pages 3-9 and 3-10).
- Select specific “from” email addresses that will be always or never sent to you (see pages 3-9).
- Select how often you receive Spam Quarantine Reports (see page 3-11). This feature is optional and may be unavailable if your Email Defense Service administrator disabled it.
- Select which emails to include in your Spam Quarantine Report (see page 3-11). This feature is optional and may be unavailable if your Email Defense Service administrator disabled it.
- Select whether your email is filtered for spam (see page 3-12). This feature is optional and may be unavailable if your Email Defense Service administrator disabled it.
Procedure

Open the Message Quarantine Window

1. To open the **Message Quarantine** window, do one of the following:
   a. When you first log into the Email Defense Portal, the **Message Quarantine** window appears by default (see “Logging into the ” on page 3-5).
   b. In the Email Defense Portal, click the **Quarantine** tab option.

The **Message Quarantine** window appears.

![Message Quarantine window](image)

**Figure 9: Message Quarantine window**

2. If desired, select another date in the Date drop-down list.
   a. Optionally, select **View all quarantined messages** to view all your quarantined spam emails.

3. If desired, click the column heading in the quarantined email list to sort by that information.
   An arrow appears in the column heading to indicate which heading and order (ascending or descending) is being used to sort the email.
   a. Optionally, click the column heading again to reverse the order of the sort.

**3.5.1. Select Which Email Address to List**

This procedure allows you to select which of your associated email addresses to view in the **Message Quarantine** window. For example, you can select to 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 to this primary email address, this feature is disabled. See “Maintaining Your Alias Email Addresses” on page 3-16 for more information about primary and alias email addresses.
Procedure

1. If available, select the desired email address in the Sent to field.
   a. Optionally, select Any of my email addresses to list all of your associated email addresses.

3.5.2. Review Single Quarantined Email

This procedure allows you to view the contents of a single email and then delete or release it. The email is opened in a “safe” window in the Email Defense Portal for your review.

Procedure

1. In the Message Quarantine window, click the email command link in the Subject column.

   The email contents open in a Safe Message View window.

   ![Safe Message View window](image)

   **Figure 10: Safe Message View window**

2. Do one of the following:
   a. To add the “from” email address to your Allow list, click the always allow button (see “Maintaining Your Allow/Deny Lists” on page 3-12 for more information).

   The email address is added to the Allow list in the Allow/Deny Sender Lists window.

   b. To add the “from” email address to your Deny list, click the always deny button (see “Maintaining Your Allow/Deny Lists” on page 3-12 for more information). This feature is optional and may be unavailable if your Email Defense Service administrator disabled it.
The email address is added to the Deny list in the Allow/Deny Sender Lists window.

c. To accept the email and have it forwarded to your primary email address, click the release button at the bottom of the Safe Message View window.

d. To delete the email, click the delete button at the bottom of the window to delete the email immediately.

3. To return to the Message Quarantine window, click the Back button on your Web browser.

3.5.3. Release Multiple Emails

This procedure allows you to release one or more emails at the same time. Released emails are sent to your primary email address.

Procedure

1. In the Message Quarantine window, select the checkbox in front of each email that you want to release.
   a. Optionally, select the checkbox next to the buttons at the bottom of the window to select all of the listed emails.

2. Click the release button at the bottom of the window to release the selected emails immediately to your primary email address.

3.5.4. Delete Multiple Emails

This procedure allows you to delete one or more emails at the same time.

1. In the Message Quarantine window, select the checkbox in front of each email that you want to delete.
   a. Optionally, select the checkbox next to the buttons at the bottom of the window to select all of the listed emails.

2. Click the delete button at the bottom of the window to delete the selected emails immediately.

3.5.5. Add Multiple Senders to Allow List

This procedure allows you to add the senders of one or more emails to your Allow list. Thereafter, all emails received from these senders' email addresses will not be checked for spam content. Another term for this process is “whitelisting." See “Maintaining Your Allow/Deny Lists” on page 3-12 for more information about managing your Allow list.

1. In the Message Quarantine window, select the checkbox in front of each email whose sender you want to add to your Allow list.
   a. Optionally, select the checkbox next to the buttons at the bottom of the window to select all of the listed emails.
2. Click the **Always Allow** button at the bottom of the window to add these senders’ email addresses to your **Allow** list.

### 3.5.6. Add Multiple Senders to Deny List

This procedure allows you to add the senders of one or more emails to your **Deny** list. Thereafter, all emails from these senders’ email addresses will never be accepted for delivery. Another term for this process is “blacklisting.” See “Maintaining Your Allow/Deny Lists” on page 3-12 for more information about managing your **Deny** list.

1. In the **Message Quarantine** window, select the checkbox in front of each email whose sender you want to add to your **Deny** list.
   a. Optionally, select the checkbox next to the buttons at the bottom of the window to select **all** of the listed emails.
2. Click the **Always Deny** button at the bottom of the window to add these senders’ email addresses to your **Deny** list. This feature is optional and may be unavailable if your Email Defense Service administrator disabled it.

### 3.5.7. Select Spam Quarantine Report Frequency

This procedure allows you to select how often you receive your Spam Quarantine Report. This feature is optional and may be unavailable if your Email Defense Service administrator disabled it.

**Important Note:** If you select **Never**, you will not receive your Spam Quarantine Reports. If the feature that allows login through the Web is disabled (see “Logging into the ” on page 3-5), you will no longer have access to the Email Defense Portal to manage your quarantined email. In this case, you must contact your Email Defense Service administrator to have this option reset and/or to have your access to the Email Defense Portal re-enabled.

1. In the **Message Quarantine** window, select the desired frequency in the **Please email my quarantine report every** field.
2. Click the **update** button next to that field.

### 3.5.8. Select Spam Quarantine Report Content

This procedure allows you to select what content you want included in your Spam Quarantine Report. This feature is optional and may be unavailable if your Email Defense Service administrator disabled it.

1. In the **Message Quarantine** window, select the desired content in the **Include the following in my report** field.
   - **All Quarantined Items** selection causes all your quarantined emails to be listed.
   - **New Items Since Last Report** selection causes only those quarantined emails that were received since your previous Spam Quarantine Report to be listed.
The **Text-only Summary** selection causes a text message to 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** window when clicked.

This option allows you to receive notifications of filtered email if your email application does not support HTML content.

- The **Default** selection causes the frequency to be set to the default configured by your Email Defense Service administrator.

2. Click the **update** button next to that field.

### 3.5.9. Turn Off/On Spam Filtering

This procedure allows you to select whether your emails will be filtered for spam content. This feature is optional and may be unavailable if your Email Defense Service administrator disabled it.

**Note:** This feature affects all your associated email addresses, including your primary address and all alias email addresses (see "Maintaining Your Alias Email Addresses" on page 3-16 for more information about alias email addresses).

1. In the **Message Quarantine** window, click to check or uncheck the **I prefer not to have my messages filtered for spam** checkbox.

2. Click the **update** button next to the checkbox description.

   a. The following occurs if you had checked the **I prefer not to have my messages filtered for spam** checkbox:
      - 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.

   b. The following occurs if you had unchecked the **I prefer not to have my messages filtered for spam** checkbox:
      - 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.

### 3.6. Maintaining Your Allow/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 using the **Message Quarantine** window (see page 3-7) or using the **Allow/Deny Sender Lists** window.
You can define a maximum of 50 email addresses in the Deny list. There is no limit to the number of email addresses in the Allow list.

**Note:** A common technique of spammers is to change their sender email address often. Be aware that your Deny list may not prevent future spams from these spammers. The Deny list primarily is used to block emails from unwanted senders.

**Definition of “Spam”**

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 emails received from recognized senders. For example, a salesman for a company may be sending you unwanted emails. In this scenario, it is unlikely that the sender address will be changed often by the spammer, so this type of address would be a good candidate to be added to Deny list.

The second type of spam includes unwanted emails containing questionable or offensive content and that are received from senders who deliberately attempt to bypass blacklisting and content filtering rules. For example, you may receive emails from a sender with a fraudulent money-making offer or containing offensive sexual content. In this scenario, these spammers often change their email addresses, email content, etc., in an attempt to bypass any blacklist filtering. This type of address is not a good candidate to be added to the Deny list because the denial will be effective for only a brief time. If this type of spam email is not filtered into your spam quarantine area, but was delivered as “normal” email, please see “Wrong Email Got Past Filter” on page 1-1 for information about how to report it.

**Procedure**

Open Allow/Deny Sender Lists Window

1. In the Email Defense Portal, click the Allow/Deny tab option.
   The Allow/Deny Sender Lists window appears.
3.6.1. Add Single Sender to Allow List or Deny List

This procedure allows you to 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.
- Use wildcards to enter a range of email address (for example, j*@abc.com) to force the emails 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:** Be aware that your Email Defense System administrator can also define **Allow** and **Deny** lists. In this case, the settings made by the administrator are applied before your settings.

**Procedure**

1. In the **Allow/Deny Sender Lists** window, type the sender address to be added in the **Add Entry** field for the appropriate list.
2. Click the **Add>>** button next to that **Add Entry** field.
   
   The email address appears in the list box.

### 3.6.2. Add Multiple Senders to Allow List or Deny List

This procedure allows you to add a predefined list of email addresses and/or domain names to your **Allow** list or your **Deny** list. The predefined list must be in the following format:

- Text file
- 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
- Use wildcards to enter a range of email address (for example, j*@abc.com) to force the emails 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. 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.

**Procedure**

1. In the **Allow/Deny Sender Lists** window, type the full path and filename of the file containing the list of email addresses to be added in the **Upload Allow List** field or the **Upload Deny List** field,
3. Optionally, click the **Browse** button to select the file.

   The **Choose file** window appears.

   1) Navigate to the file location, click to select the file, and click the **Open** button.

2. Click the appropriate **Upload File** button.

   The addresses from the file appear in the appropriate list.

### 3.6.3. Remove Senders from Allow List or Deny List

This procedure allows you to remove sender addresses from your **Allow** or **Deny** list.

**Procedure**

1. In the **Allow/Deny Sender Lists** window, click to select the sender address in the appropriate list box.

   a. Optionally, press and hold the <Shift> or <Ctrl> keys while clicking to select multiple email addresses.

2. Click the **Remove** button next to the list box where the sender addresses are selected.

   The selected sender addresses disappear from the list box.

### 3.7. Maintaining Your Alias Email Addresses

#### Primary vs. Alias Email Addresses

You must have a primary email address defined in the Email Defense Service to log into the Email Defense Portal, to have email filtered for spam, viruses, etc., and to receive a Spam Quarantine Report. Your primary email address may have been defined by your Email Defense Service administrator or the Email Defense Service may have defined one for you automatically when it received emails to your address.

You may have multiple primary email addresses, depending on whether you have been using multiple email addresses in the Email Defense Service. In this case, you would have multiple quarantine areas that you must log into 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 alias email addresses. The maximum allowed number of alias email addresses is configured by your Email Defense Service 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 Email Defense Service 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, the Email Defense Service automatically created the appropriate alias email addresses based on your primary email address using that alias domain name. These addresses are listed for your information and are automatically aliased to your primary email address.

This feature is optional and would be unavailable if your Email Defense Service administrator disabled it.

**Quarantined Emails**

You would have one quarantine area to manage for each set of associated email addresses. You would receive one Spam Quarantine Report including 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 emails released from the quarantine area are sent to the primary email address. For example, if an email is quarantined and then released that has a recipient address that is an alias email address, it is sent to the primary email address.

**User Configurations**

All the associated email addresses, primary and aliases, would be controlled by the primary email address' user configuration (for example, allow and deny lists) in the Email Defense Service.

**Adding Alias Email Addresses**

If you add an alias email address in the **User Aliases** window in the Email Defense Portal, the following occurs:

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

B. 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 Primary to Alias Email Address” on page 3-18.

C. Thereafter, the alias email address' quarantine information will be combined with 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:

A. If the email address that received the Spam Quarantine Report already has alias email addresses, the Email Defense Portal is opened to the **Configuration – User Aliases** window in your local browser. You can then perform your alias email address management.
B. If the email address that received the Spam Quarantine Report does not already have alias email addresses, the Email Defense Portal is opened to a window that prompts you for your primary email address (the email address to which you want to associate alias email addresses).

1. An email is sent to that primary address to confirm that you are authorized to change its use.

2. Once the recipient clicks the authorization command in the email in his/her local email application, the Email Defense Portal is opened to the Configuration – User Aliases window in his/her local browser.

3. The recipient can then perform your alias email address management.

Converting Primary to Alias Email 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 address 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 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 (“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 Email Defense Service administrator can delete primary 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. (see "Converting Primary to Alias Email Address" on page 3-18 for more information about converting a primary email address to an alias 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).

The Configuration – User Aliases window is the location where you manage your alias email addresses. In the Configuration – User Aliases window, 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
Procedure

Open Configuration – User Aliases Window

1. To open the **Configuration – User Aliases** window, do one of the following:
   a. Log into the Email Defense Portal (see page 3-5).
      1) Click the **Setup** tab option.
      2) In the **Configuration – Password Change** window, click the **Aliases** menu option.
      The **Configuration – Aliases** window appears.
   b. In the Spam Quarantine Report, click the **Manage My Email Addresses** command link.
      1) If you currently have alias email addresses defined, the **Configuration – Aliases** window appears.
      2) If you do not have alias email addresses defined, the **Configuration** window appears and prompts you for your primary email address.
         a) Type your email address and click the **Submit** button.
         b) An authorization email is sent automatically to the entered email address requesting authorization for the change.
         c) The recipient of the email must click the authorization link in his/her local email application to continue the process to change the email address.
         d) Immediately after the Email Defense Service receives the authorization, a Web browser is opened on the recipient’s local machine, the Email Defense Portal is initiated, and user is automatically logged in for the email address that was saved in the command.
      The **Configuration – Aliases** window appears.
3.7.1. Select Which Email Address is Primary

If you already have alias email addresses associated with your primary email address, this procedure allows you to 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 Email Defense Service 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.

Procedure

1. In the Configuration – Aliases window, click the selection 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.

3.7.2. Add an Alias Email Address

This procedure allows you to 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.

Procedure

1. In the Configuration – Aliases window, type the email address to be added as an alias email address in the Add an Alias Email Address for {primary address} field, where {primary address} is the current primary email address,
   a. If necessary, select a domain in the Domain field to the right of @ character.

   This field appears only if your domain has alias domain names associated with it.

2. Click the Add button.

3. An authorization email is sent automatically to the added email address requesting authorization for the change.

4. The recipient of the email must click the authorization link in his/her local email application to continue the alias addition.

5. Immediately after the Email Defense Service receives the authorization, the email address is added as an alias email address to the listed primary email address.
3.7.3. Delete an Alias Email Address

This procedure allows you to delete an alias email address, which removes its association with the primary email address. If you continue to receive email to the deleted address, the Email Defense Service will recreate the email address as a primary email address with default user configurations. You cannot delete a primary email address (see “Deleting Associated Email Addresses” on page 3-18 for information about deleting alias email addresses).

Procedure

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. In the Configuration – Aliases window, click the Delete button next to the alias email address that you want to delete.

   **Note:** The email address is deleted *immediately* after you click the Delete button.