SecurityGateway

Quarantine Management - Best Practices

SecurityGateway's flexible quarantine configuration options can be configured to hold quarantined messages on the server, or to allow the mail server or client to filter quarantined messages. When quarantined messages are held on the server, administrators can grant users access to manage their own quarantines.

There are two ways users can manage their quarantines - via the quarantine summary email that is sent out periodically, or via the SecurityGateway interface. This guide provides instructions for both methods.

Via the Quarantine Summary Email

The SecurityGateway administrator can configure how often users receive an email listing the contents of their quarantine folder. For each quarantined message, users can release the messasge for delivery, always allow email from the sender, or blacklist the sender. Each option is explained below.

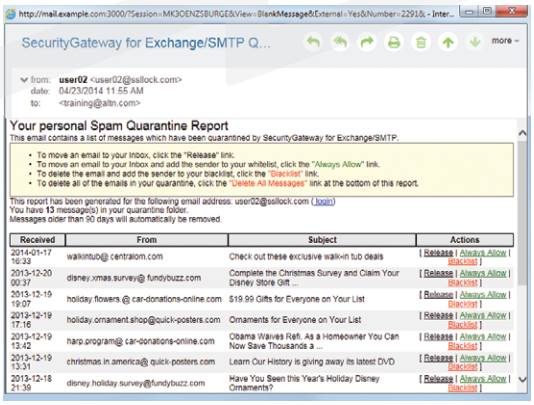

Figure 1-1

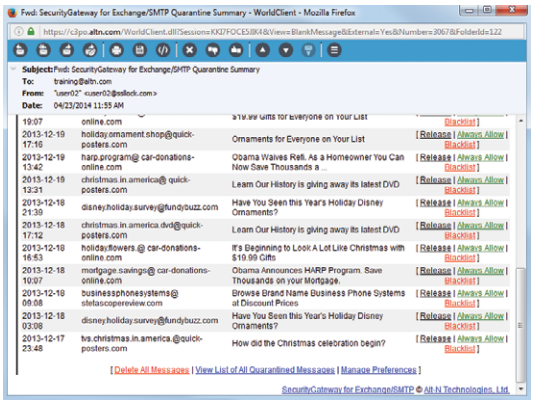

Figure 1-2

1. **Release** - Click on Release to release the message from the quarantine & deliver it to your Inbox. [Figure 1-1]
2. **Always Allow** - If you do not want to block messages from this sender, you can select Always Allow to add the sender to your whitelist. When this option is selected, messages from the sender will never be quarantined. [Figure 1-1]
3. **Blacklist** - This option adds the sender to your blacklist. All messages from blacklisted senders will be blocked. Use this feature with caution. SecurityGateway is able to more accurately detect spam if you teach it what is and is not spam through the use of the "Spam" and "Not Spam" buttons. This must be done when logged into the SecurityGateway user interface. In addition, if a legitimate address ends up being blacklisted by mistake, messages from that address will be rejected. If this happens, you will need to ask the sender to resend the message. [Figure 1-1]
4. Click on **Delete All Messages** to permanently remove all messages from your personal quarantine. [Figure 1-2]
5. When you click on **View List of All quarantined messages**, you will be taken to your quarantine within the SecurityGateway interface. [Figure 1-2]
6. Click on **Manage Preferences** to modify your quarantine preferences. [Figure 1-2]
7. Use the **Login** link at the top to log into SecurityGateway.

Via the SecurityGateway Interface

In addition to managing their quarantines from the Quarantine Summary email, users who have been granted permissions to manage their own quarantines can view their quarantined messages directly in SecurityGateway.

Before users can access their quarantines in SecurityGateway, the administrator will need to grant them permission to manage their quarantines, as outlined in the following steps:

1. Click on the **Setup / Users** tab.
2. Click on **Quarantine Configuration** under the **Mail Configuration** section. [Figure 2-1]
3. Check the box **Allow users to view & manage their own quarantine folders**.
4. Click on **Save**.

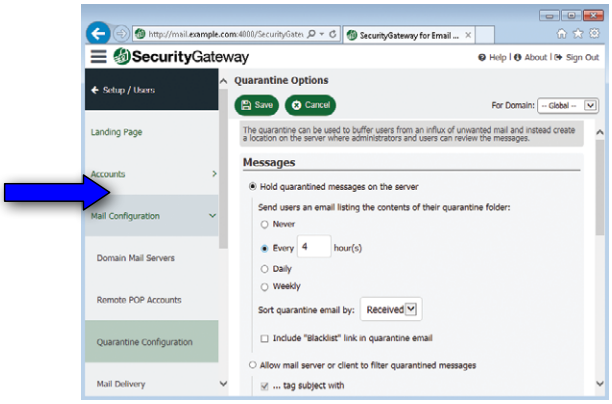

Figure 2-1

Users can access their quarantines via the **View My Quarantine** link on the left-hand side of the SecurityGateway dashboard. The options across the top of the quarantine allow users to refresh the message list, search for messages based on specific criteria, view a message, release a message for delivery, delete the message, mark the message as spam or non-spam, or whitelist or blacklist the sender or sender's domain. These options are explained in more detail below.

Figure 2-2

1. Click on **Refresh** to refresh the list of messages in your quarantine. [Figure 2-2]
2. Use the **Search** button to search the contents of the quarantine based on specific criteria. You can search for a message based on whether it was inbound or outbound, the contents of the From, Subject or Recipient header, the date the message was received, and the reason the message was quarantined. [Figure 2-3]
3. Clicking on **View** displays the message in a separate window where you can view the message transcript, the actual message, or the message source. These options are useful for troubleshooting purposes. [Figure 2-2]
4. Click on **Release** to release the message from the quarantine and deliver it to its intended recipient. [Figure 2-2]
5. Click on **Delete** to delete the message from your quarantine. [Figure 2-2]
6. For quarantined messages that are determined to be spam, click on the **Thumbs-Down** icon to mark the message as spam. [Figure 2-2]
7. For false-positives (legitimate, non-spam messages that are marked as spam) click on the **Thumbs-Up** icon to mark the message as non-spam. [Figure 2-2]

   Note: Using the thumbs-up and thumbs-down icons helps train the spam filter to be more accurate over time, and is more effective than blacklisting the sender.

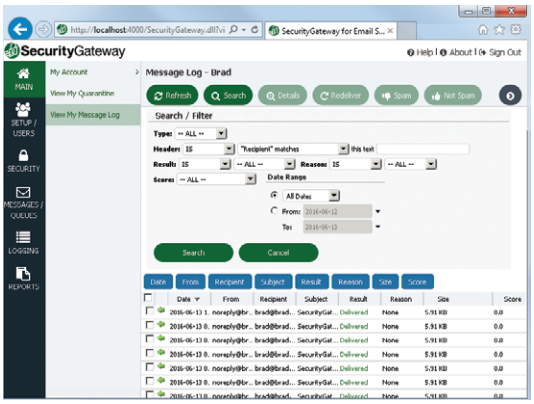

Figure 2-3

8. Use the **Whitelist** button to accept all messages from the sender or the sender's domain. [Figure 3-1]
9. Use the **Blacklist** button to block all messages from the sender or the sender's domain. *Use this feature with caution. SecurityGateway is able to more accurately detect spam if you teach it what is and is not spam through the use of the "Spam" and "Not Spam" buttons as explained in Steps 6 and 7. This must be done when logged into the SecurityGateway user interface. In addition, if a legitimate address ends up being blacklisted by mistake, messages from that address will be rejected. If this happens, you will need to ask the sender to resend the message.* [Figure 3-2]

   *Note: Blacklist behavior is determined by settings under **Security | Blacklist | Action**. On this screen, you have two options - refuse the message or quarantine the message.*

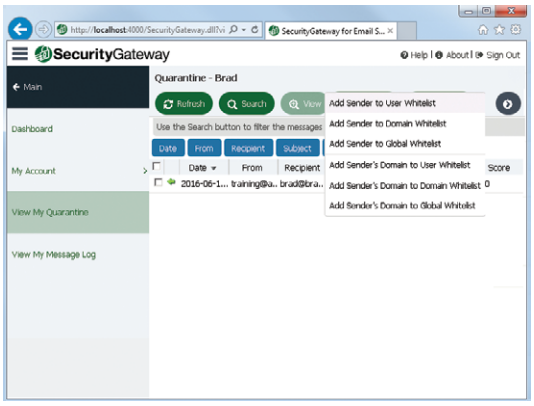

Figure 3-1

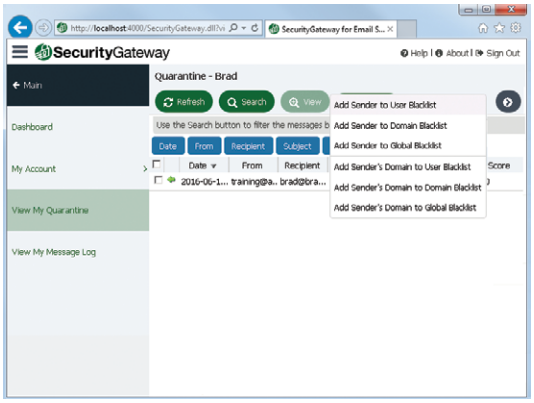

Figure 3-2