

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 blocklist the sender (depending on which permissions the administrator has enabled for the user). Each option is explained below.

- 1. Release Click on Release to release the message from the quarantine & deliver it to your Inbox. [Figure 1-1]
- Always Allow If you do not want to block messages from this sender, you can select Always Allow to add the sender to your allow list. When this option is selected, messages from the sender will never be quarantined. [Figure 1-1]
- 3. Blocklist This option adds the sender to your blocklist. All messages from blocklisted 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 blocklisted 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.

| date: 0 | ecurityGateway for Email Se 2/14/2019 11:00 AM rank Thomas <frank:thomas@< th=""><th>ervers <noreply@brad.ssllock.com> brad.ssllock.com></noreply@brad.ssllock.com></th><th></th></frank:thomas@<> | ervers <noreply@brad.ssllock.com> brad.ssllock.com></noreply@brad.ssllock.com> | |
|--|--|--|--|
| | Your | personal Spam Quarantine Rep | ort |
| This email c | ontains a list of messages which | have been quarantined by SecurityOateway for Err | sail Servers. |
| To d | | n As Spam" link. Ser to your blacklist, click the "Blacklist" link. | |
| This report h You have 8 n | | | |
| This report h You have 8 n | as been generated for the follow | ing email address: "Frank Thomas" frank.thomasg Ider. | |
| This report h You have & n Messages o | as been generated for the follow nessage(s) in your quarantine fol Ider than 30 days will automatica Frem | ing email address: "Frank Thomas" frank.thomas@ 1946. Ny be removed. | (brad sollock.com (<u>cojn</u>) |
| This report h You have 0 m Messages o Received 2019-02-14 | as been generated for the follow nessage(s) in your quarantine fol ider than 30 days will automatica Frem | ing email address: "Frank Thomas" frank thomasg Iše: Ity be removed. Subject You're going to LOVE our OISC Lunch Keynote | Brad ssilock.com (cojn) Actions [Eleisade Award Alizer Confirm As |
| This report h You have 8 m Messages of Received 2019-02-14 09:04 2019-02-13 | as been generated for the follow nessage(ii) in your quarantine fol ider than 30 days will adomatica From malbers@technologyfirst.org jodi.szimanski@zwaterioo.ca | ing email address. "Frank Thomas" frank thomas (set the removed. Subject Youne going to LOVE our OISC Lunch Keynole Speaked | Read sellock com (ppp) Actions [Release Award Allow Confirm As Balan Balacita] [Release Award Allow Confirm As |
| This report h You have the Messages of Received 2019-02-14 09:04 2019-02-13 11:49 2019-02-13 | as been generated for the follow nessage(s) in your quarantine fol ident han 30 days will automatica Frem malbers @technolognfirst.org jodi.szimanski@zwaterloo.ca news@tophos.com | ing email address. "Frank Thomas" frank thomas (56) hy be removed. Subject Youhe going to LOVE our OISC Lunch Keynole Opeaker Find NewBit online | Actions Actions [Briess Altern (Confirm As Batter (Backbar) [Briess (Annum Altern (Confirm As Batter (Bliess)] [Briess (Annum Altern (Confirm As Batter (Bliess)] |

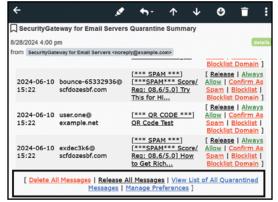


Figure 1-2

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.

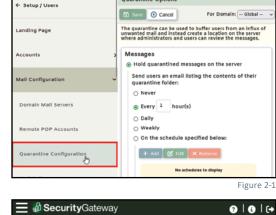
Before users can access their guarantines in SecurityGateway, the administrator will need to grant them permission to manage their quarantines, as outlined in the following steps:

- 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.

Users can access their guarantines via the View My Quarantine link at the top of the SecurityGateway dashboard (or in the side panel for smaller screens). The options available 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 (if the administrator has enabled user permissions to perform these actions), or allowlist or blocklist the sender or sender's domain. These options are explained in more detail below.

- 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 guarantine 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 guarantine and deliver it to its intended recipient. [Figure 2-2]
- 5. Click on **Delete** to delete the message from your guarantine. [Figure 2-2]
- 6. For guarantined 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 blocklisting the sender.



Quarantine Option:

📃 ऺ SecurityGateway

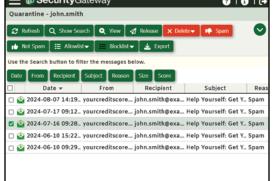
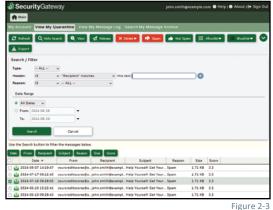


Figure 2-2



⑦ | ③ | G

- 8. Use the Allowlist button to accept all messages from the sender or the sender's domain. [Figure 3-1]
- 9. Use the Blocklist 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 blocklisted 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: Blocklist behavior is determined by settings under **Security / Blocklists / Configuration**. On this screen, you have two options - refuse the message (and optionally disconnect from the sending server) or quarantine the message. These settings can be configured globally or per-domain.





Figure 3-2



© 1996 - 2024 MDaemon Technologies, Ltd.

MDaemon, RelayFax, and SecurityGateway are trademarks of MDaemon Technologies, Ltd. All trademarks are property of their respective owners. 8.29.2024