Understanding the Message Log

https://campus.barracuda.com/doc/96023047/

The Message Log is a log of all inbound and outbound messages that are sent to and from your domain(s), regardless of whether they were delivered. Each time an attempt is made to send mail to or from your domain(s), it is recorded in the Message Log. For example, if a message sent to your domain is deferred, it appears in the Message Log as *Not Delivered*. If and when the sending server retries this message, a new entry appears in the Message Log. The original entry and delivery status in the message log does not change. A new entry appears each time. Therefore, there might be multiple entries/attempts to deliver the same email and each of these entries might have a different delivery status and different message ID.

> The Message Log is not an inbox. It is a log of all entries. Therefore, messages cannot be deleted from the message log.

The Message Log is a window into how the current spam, virus, and policy settings are filtering email coming through Email Gateway Defense. Use the information in the log to help tune your inbound and outbound policy settings. The Reading Pane is hidden by default, enabling you to quickly scan through messages. Select **Right**, **Bottom**, or **Off** to change the reading pane.

Note that messages are deleted after 30 days.

> If you make setting changes, allow a few minutes for the changes to take effect.

The Message Log reflects all email traffic through Email Gateway Defense at the global level. If you click on a verified domain on the **Domains > Domain Manager** page, a tab for the Message Log for that domain displays. Additionally, you can track end-user quarantine notifications in the Message Log.

> All messages going through Email Gateway Defense are subject to a size limit of 300MB. This includes headers, body, and any attached content.

Filter the Message Log

When viewing the global Message Log, you can choose to view only **Inbound** or only **Outbound** mail using the Message Log **Filter**. You can filter on **All**, **Allowed**, **UI Delivered**, **Email Continuity**, **Not Allowed**, **Blocked**, **Deferred**, or **Quarantined** messages. For details on each of these actions, see Message Actions. Filter messages using the Advanced Search feature to quickly view email by

allowed, deferred, quarantined, encrypted (outbound), or blocked messages by domain, sender, recipient, time range (last 2- 30 days), envelope to, envelope from, reason, action taken (see Message Actions), date or subject.

The User Message Log is less comprehensive than the global, administrator's Message Log. For example, users cannot see outbound mail in their Message Log.

> For more information about filtering messages, see Filtering the Message Log. You can also click the **Help** icon on the **Message Log** page at the global level or after logging into a User account.

Create Saved Searches

You can save a search so it is convenient to use in the future.

To create a saved search:

1. Do one of the following:
   - Enter a search term in the **Search** box, then click **Search**.
   - Click **Advanced Search**, enter one or more search terms, then click **Search**.
2. Click **Saved Searches**. In the blank space, type a name for your search, then click **Save**. Confirm you see the search you just created in the list.
3. When you are ready to run a saved search, click **Saved Searches**, then click the name of that saved search.

To delete a saved search, in the **Saved Search** panel, click **Remove**.

Incorrectly Blocked or Incorrectly Delivered Messages

Occasionally Email Gateway Defense might incorrectly identify a piece of mail as Spam (false positive) or Not Spam relative to the policies you have set. You can tune the **Advanced Spam Detection Scoring** levels on the **Inbound Settings > Anti-spam Antivirus** page by selecting **Custom** and adjusting the score for each category based on what type of mail you consider to be spam.

Occasionally, Email Gateway Defense might incorrectly block or allow a message based on Barracuda Networks settings. Reporting these messages helps improve spam detection. Use the following buttons on the Message Log page (both at the global level and the user account level) to mark a

message and have it sent to the Barracuda Networks team for further review.

When you report a message as incorrectly blocked or incorrectly delivered, in addition to the submission confirmation, you will also be asked to provide additional details as to why you think that message was incorrectly delivered or incorrectly blocked. If you choose to provide these details, you will be redirected to a feedback response form to select a reason from a list of options or to type in a reason. Your feedback is extremely important to us. Providing additional details will help us improve our systems and allow better understanding of your email preferences.

Note that reporting this message does not automatically block or deliver all messages from this sender. To immediately allow or block certain email addresses or domains, you can create a sender policy on the **Inbound Settings>Sender Policies** page.

- **Report as Incorrectly Blocked** – Message should have been delivered. This includes messages that are not spam.
- **Report as Incorrectly Delivered** – Message should have been blocked. This includes spam messages.

Incident Response Users: Messages you mark as **Incorrectly Delivered** appear in the User-Reported Emails page, where they can be investigated and remediated if needed.

Deliver Messages to Recipient

You can click **Deliver** for one or more selected messages in the Message Log if you decide the message is valid.

- *If a message is successfully delivered*, a new message entry appears in the Message Log with the **Delivery Status** of **UI Delivered**.
- *If a message cannot be delivered*, you are notified by a message in your browser. A new message entry appears in the Message Log with the **Delivery Status** of **Not Delivered**.

If the **Reason** field for a blocked message displays as **Advanced Threat Protection**, you cannot immediately deliver the message. See Advanced Threat Protection Reports for details.

If delivered messages are not making it to the recipient's mailbox, it may be due to a filter on your mail server or a service on your network catching the mail as spam. Check your local trash/spam folder to locate the mail.

User's Message Log
Individual users have an additional option to remove selected messages from their personal

Message Log. The user can select one or more messages, and click **Delete**.

Message Details

Click on a message in the table and its Action and Reason display below. Click **Show Details** in the message header to view additional information including IP address, recipients, and delivery status. The administrator (or user, when viewing their own account) can then elect to View the entire message and take actions on the message. The words **Includes Other Recipients** in the Message Details link indicate that the message was sent to multiple recipients or distribution lists. The individual addresses are listed in the message details.

If your Message Log shows an email message with a subject of **Message has no content**, this is due to a failed connection. Email Gateway Defense now logs all failed connections. The record for a failed connection shows the from/to data, but the log entry does not have any header or body content. As a consequence, mail that is malformed or is addressed to an invalid recipient displays in the logs with the **Message has no content** in the Subject line.

Message History

Each record in the message log represents a separate event. For example, if a message is not initially delivered, but is successfully delivered later, there are at least two events – one for the initial error and another for the delivery – and possibly additional events for retrying the delivery. It can be helpful to see all of the events related to a single record in one place.

The **Show Message History** button displays in the Reading pane. The Reading pane control is at the top of the Message Log. Select **Right** or **Bottom** to choose where you want the Reading pane to display.

To view all events associated with a single record:

1. Select a record.
2. In the **Reading** pane, click **Show Message History**.
    - The Message Log populates with all records related to the original record you selected.
    - If the record has no content, as described in the note above, **Message has no content** displays and **Show Message History** does not display.
    - If there are no related records, only the record that you selected appears in the Message Log.
3. Optionally, click **Hide Message History** to return to the Message Log.

Investigating and Remediating Emails

This feature is available if you are using Incident Response and have at least one Microsoft 365 account associated with Barracuda Email Protection.

If you find a questionable email in the message log, you can move seamlessly from Email Gateway Defense to Incident Response to investigate it.

To find messages similar to the questionable email:

1. Log into Email Gateway Defense as an administrator.
2. In the Message Log, find the questionable email and click it to view its details.
3. Click **Search for similar messages**. The Incident Response wizard opens in a new browser tab.
4. Continue with the wizard, as described in Creating an Incident. Note that the fields in the wizard are pre-populated with the information from the email in the message log.

With Incident Response, you can find similar emails, then if needed, take action to remediate any issues, including removing emails from users' mailboxes and creating policies to block senders. Refer to Incident Response Overview for details.