Message Actions

https://campus.barracuda.com/doc/96023048/

Table 1 describes the actions Email Gateway Defense takes with messages on the **Overview > Message Log** page.

Table 1. Message Reasons and Actions

Reason	Action and Description
Account Suspended	If your Email Gateway Defense subscription expired more than 60 days ago, your account is marked as **Suspended**, and email are no longer scanned for spam. Note: Email is still scanned for viruses.
Advanced Threat Protection	Message blocked by the Advanced Threat Protection (ATP) cloud-based virus scanning service. ATP is an advanced virus scanning service which, when enabled on the **ATP Settings** page, provides additional scanning for the attachment file types you specify. **See also**: • Understanding Advanced Threat Protection Reports • Advanced Threat Protection Reports
Anti-Fraud	Barracuda Anti-Fraud Intelligence detected a potential phishing scheme, which could be used to gather confidential information about an organization or its individual users.
Antivirus	The message had a virus attached.
Attachment Content	Content in a message attachment matched a **Message Content Filter** rule specified on the **Inbound Settings > Content Policies** page.
Attachment Filter	Content in a message attachment matched an attachment filter defined on either the **Inbound Settings > Content Policies** or the **Outbound Settings > Content Policies** page.
ATP Exempt	Message was exempted by ATP scan.
ATP Scan Inconclusive	Message was quarantined because the ATP scan timed out or resulted in an unknown response.
AV Service Unavailable	The **Scan Email for Viruses** setting on the **Inbound Settings > Anti-Spam/Antivirus** page is set to **Yes**, but the virus scanning service was temporarily unavailable when the message came through. Note: The message is deferred and retried when the virus scanning service is available.
BRTS	Barracuda Real-Time System (BRTS) detected a zero-hour spam or virus. This advanced service detects spam or virus outbreaks even where traditional heuristics and signatures to detect such messages do not yet exist.

Barracuda Reputation	Message was sent from a particular IP address on the Barracuda Reputation Block List (BRBL). A list maintained by Barracuda Central that includes IP addresses of known spammers.
Body Content	Message body content matched a **Message Content Filter** rule specified on the **Inbound Settings > Content Policies** page.
Bulk Email	The **Bulk Email Detection** setting on the **Inbound Settings > Anti-Spam/Antivirus** page is set to **Yes**, and the message qualifies as **Bulk**.
Cloudscan Service Unavailable	The **Enable Cloudscan** setting on the **Inbound Settings > Anti-Spam/Antivirus** page is set to **Yes**, but the Cloudscan spam scoring service was temporarily unavailable when the message came through. Note: The message is deferred and is retried when the Cloudscan service is available.
Content Protected	The message has a password-protected archive attachment. See settings for **Attachment Filter** on the **Inbound Settings** > **Content Policies** and **Outbound Settings > Content Policies** pages.
Content URL	The message contained one or more URLs listed in the **Intent Domain Policies** section on the **Inbound Settings > Anti-Phishing** page.
DKIM	The **DomainKeys Identified Mail (DKIM)** setting on the **Inbound Settings > Sender Authorization** page is set to **Quarantine** or **Block** and the message is from a domain that fails DKIM verification.
DMARC	**The Domain Based Message Authentication (DMARC)** setting on the **Inbound Settings > Sender Authorization** page is **Enabled** and the message is from a domain that fails DMARC verification.

Email Categorization	Per settings on the **Inbound Settings > Anti-spam/Antivirus** page, email from this sender is categorized as not necessarily spam, but rather something that the user may have subscribed to at one time and may no longer wish to receive. For example, newsletters and memberships, or marketing information. Categories supported appear in the Message Log **Reason** as: • **Email Categorization (corporate)** Emails sent by a user at an authenticated organization from an MS Exchange Server that involves general corporate communications. Does not include marketing newsletters. • **Email Categorization (transactional)** Emails related to order confirmations, bills, invoices, bank statements, delivery/shipping notices, and service-related surveys • **Email Categorization (marketing)** Promotional emails from companies such as Constant Contact • **Email Categorization (mailing lists)** Emails from mailing lists, newsgroups, and other subscription-based services such as Google and Yahoo! Groups • **Email Categorization (social media)** Notifications and other emails from social media sites such as Facebook and LinkedIn. Email Categorization assigns some of these emails to specific categories which the admin can set to allow, block, or quarantine on the **Inbound Settings > Anti-spam/Antivirus** page.
Extortion	Message blocked by Machine Learning. Attackers leverage usernames and passwords stolen in data breaches, using the information to contact and try to trick victims into giving them money.
From Address	A sender or content rule for **From Address** was encountered.
GeoIP Policies	Message blocked/quarantined based on a country of origin policy selected on the **Inbound Settings > Regional Policies** page.
Header Content	Content in the message header matched a Message Content Filter rule specified on the **Inbound Settings > Content Policies** page.
IP Address Policies	The sending IP address is listed as **Blocked** or **Exempt** on the **Inbound Settings > IP Address Policies** page.
Image Analysis	Image Analysis identified this message as a bulk/spam message.
Inbound TLS Required	On the **Domains > Settings** page, the setting **Require TLS to Barracuda from these domains** lists domains that must use a TLS connection when connecting to Email Gateway Defense. If a TLS connection was not used, then the inbound message is blocked with a reason of **Inbound TLS Required**.
Intent Analysis	Intention Analysis identified this message as a bulk/spam message.
Invalid Recipient	The **To** address does not exist on the mail server.
Language Policies	Message blocked/quarantined based on the selected character class on the **Inbound Settings > Regional Policies** page.

Malformed	The message did not conform to the SMTP protocol; for example, the **Sender**, **From**, **Date**, or other required fields may be empty.
Message Delivery Interrupted	This error occurs when a sender's connection drops during email transmission, or if a sender closes or quits their email editor before email transmission is complete. The message is deferred until the connection resumes and the email is successfully sent.
Message Too Large	The message exceeded the maximum message size allowed by the destination mail server, which rejected the message. Email Gateway Defense allows messages of up to 300 MB.
No PTR Record	Action was taken because: (1) The Block on **No PTR Records** setting on the **Inbound Settings > Sender Authentication** page was set to **Yes**, and b ecause of (1), Email Gateway Defense queried DNS for the SPF record of the sending domain, and no PTR record was found.
Office Protected	The message has a password-protected Microsoft Office attachment. See settings for **Attachment Filter** on the **Inbound Settings > Content Policies** and **Outbound Settings > Content Policies** pages.
Password Protected PDF Filtering	The message has a password-protected PDF attachment. See settings for **Attachment Filter** on the **Inbound Settings > Content Policies and Outbound Settings > Content Policies** pages.
Pending Scan	When ATP is enabled with the **Scan First, Then Deliver** option, the message is deferred because attachment scanning is pending. The mail server retries later to check if the scan is complete and, if it is, delivers the message.
Phishing	Message blocked by Machine Learning. Messages sent directly to victims to enter sensitive information such as usernames, passwords, or banking details, on a fake website that looks like a legitimate website. Cybercriminals often use that sensitive information for malicious use.
Possible Mail Loop	IP address for the destination mail server is not correctly configured in Email Gateway Defense, and may instead contain the IP address for Email Gateway Defense, causing a mail loop.
Predefined Attachment Content	An attachment contained content that matched a Predefined filter based on data leakage patterns (specific to United States). See the **Outbound Settings > Content Policies** page.
Predefined Body Content	The message body contained content that matched a predefined filter based on data leakage patterns (specific to United States). See the **Outbound Settings > Content Policies** page.
Predefined Filter Exceptions	The message body contained content that matched a predefined filter exception to HIPAA or Privacy content filters. See the **Outbound Settings > Content Policies** page.
Predefined From Address	The message **From** address contained content that matched a predefined filter based on data leakage patterns (specific to United States). See the **Outbound Settings > Content Policies** page.

Predefined Header Content	The message header contained content that matched a predefined filter based on data leakage patterns (specific to United States). See the **Outbound Settings > Content Policies** page.
Predefined Subject Content	The message subject contained content that matched a predefined filter based on data leakage patterns (specific to United States). See the **Outbound Settings > Content Policies** page.
Predefined To/CC Address	The message **To/CC** address contained content that matched a predefined filter based on data leakage patterns (specific to United States). See the **Outbound Settings > Content Policies** page.
Rate Control	Sender IP address exceeded maximum number of allowed connections in a half-hour period. Note: The message is deferred unless the client continues to make connections.
Realtime Block List	IP Reputation Analysis determined that the sending IP address is listed on a Real-Time Block List (RBL) or DNS Block List (DNSBL).
Recipient	Action was taken because of a rule for the **To** address.
Remediated by Incident Response	Incident Response remediated this email by deleting it from recipient's inbox.
Remediated by Impersonation Protection	Impersonation Protection remediated this email either by deleting it from the recipient’s inbox or by moving it to the recipient's Junk mailbox.
Score	The message score exceeded the **Cloudscan Scoring** setting on the **Inbound Settings > Anti-Spam/Antivirus** page.
Security Awareness Training	Message was sent as part of a Security Awareness Training campaign.
Sender Email Address	The message was blocked for sender email address. This sender is listed in the Barracuda email block list.
Sender Policies	Action was taken because of settings configured on the **Inbound Settings > Sender Policies** page.
Sender Policy Framework (SPF)	The Sender IP address is not listed as an allowed sender for the specified domain using the SPF protocol.
Sender Spoof Protection	Action was taken because of a rule to block the "From" address that uses your domain.
Spam	Message blocked by Machine Learning. Unsolicited bulk email messages, also known as junk email. Spam comes in various forms. Some spam emails push scams. Others are used to conduct email fraud. Spam also comes in the form of phishing emails that use brand impersonation to trick users into revealing personal information, such as login credentials and credit card details.

Subject Content	Content in the **subject** line matched a Message Content Filter rule specified on the **Inbound Settings > Content Policies** page. Note: A subject line of **Message Has No Content** indicates an incomplete SMTP transaction due to a failed connection. The log entry shows the from/to data, but has no header or body content. This mail includes messages that are malformed or are addressed to invalid recipients.
Suspicious	Message deferred or blocked due to multi-level intent checks or Barracuda Anti-Fraud Intelligence checks, as configured on the **Inbound Settings > Anti-spam/Antivirus** page. If the sending server retries the message, which indicates the message is most likely not from a spammer, Barracuda Networks will allow the message, When an email is blocked as suspicious and the mail is legitimate, contact Barracuda Networks Technical Support to let our spam accuracy team know to remove the domain from the intent/suspicious listing. For mail deferred as suspicious, Barracuda Networks can turn off the suspicious filter upon request. Note that this is not recommended as it can allow more spam to pass through.
System Sender Policies	The sender has been blocked per policy set by Barracuda Networks; this action prevents Email Gateway Defense IP address from being blocked. Contact your email administrator if you have questions. Note: Applies to outbound mail.
TLS Required	On the **Outbound Settings > DLP/Encryption** page, a TLS connection must be used when connecting to the recipient domains listed. If a TLS connection cannot be established, then the outbound message is not delivered and is blocked, with a reason of **TLS Required**.
To/CC Address	Action was taken because of a recipient or content rule for **To/CC Address**.
UI Delivered	For emails blocked or quarantined in the Message Log, the admin can manually deliver those messages. Once the message is delivered, the reason code for that message displays as **Allowed** with a reason of **UI Delivered**.

When searching for messages in the Message Log, you can use the filters listed in Table 2.

Table 2. Search Filters.

Filter	Description
Inbound Mail	
Allowed	Search for delivered messages.
Not Allowed	Search for undelivered messages. To further refine your search, select **Blocked**, **Deferred**, or **Quarantined**.
Blocked	Search for blocked messages. Messages are blocked due to a policy specified on the **Inbound Settings** and **Outbound Settings** pages.

Deferred	Search for deferred messages. Indicates that Email Gateway Defense returned a 4xx response to the sending mail server. There are several reasons for deferring messages: • The destination mail server was offline. For inbound email, if Spooling is enabled, then the messages would be spooled and *not* deferred, until the server is reachable. See *Email Spooling* below for more information. • The recipient was not valid. • The destination mail server returned a 4xx response (try later). • Rate control. See Inbound Rate Control for how rate control is applied to inbound email. • The administrator can *decide* to defer messages per policy regarding **Content Intent** on the **Inbound Settings > Anti-Spam/Antivirus** page. When a message is deferred due to intent, if the sender retries the message, it is allowed and delivered to the recipient.
Quarantined	Search for quarantined messages. Messages are quarantined due to policies specified on the **Inbound Settings and Outbound Settings** pages.
Outbound Mail	
Allowed	Search for delivered messages.
Not Allowed	Search for undelivered messages. To further refine your search, select **Blocked**, **Deferred**, or **Quarantined**.
Blocked	Search for blocked messages. Messages are blocked due to policies specified on the **Inbound Settings and Outbound Settings** pages.
Deferred	Search for deferred messages. Indicates that Email Gateway Defense returned a 4xx response to the sending mail server. There are several reasons for deferring messages: • The destination mail server was offline. • The recipient was not valid. • The destination mail server returned a 4xx response (try later). • Rate control. See Inbound Rate Control for how rate control is applied to outbound email. • The administrator can *decide* to defer messages per policy regarding **Content Intent** on the **Inbound Settings > Anti-Spam/Antivirus** page. When a message is deferred due to intent, if the sender retries the message, it is allowed and delivered to the recipient.
Quarantined	Search for quarantined messages. Messages are quarantined due to policies specified on the **Inbound Settings and Outbound Settings** pages.
Encrypted	Search for encrypted messages. The Barracuda Email Encryption Service encrypts messages due to policy as specified in the **Inbound Settings and Outbound Settings** pages. Email Gateway Defense sends the message recipient(s) a notification email directing them to visit the Barracuda Message Center to retrieve the encrypted message.
Rejected	Search for rejected messages.

Email Spooling

You can enable **Spooling** if you want Email Gateway Defense to retain all of your email for up to 96 hours if your mail server goes down. Select **Yes** to enable or **No** to disable. If Spooling is set to **No** and the service cannot connect to your mail server, the mail is deferred and the **Delivery Status** in the Message Log displays as **Not Delivered**. The sending mail server, depending on its configuration, has the option of retrying the message or notifying the sender that the mail was deferred or failed.