

## Describe why a message was rejected or temporarily reje...

Author:  
Webservio Inc.

Created On: 11 Feb 2013 7:40 PM

---

In our web-interface, we use different classifications to describe why a message was rejected or temporarily rejected.

### Temporarily Rejected (4xx SMTP response)

#### **TEMPORARILY REJECTED**

Messages which have been temporarily rejected, stay stored on the sending mail server. Legitimate mailservers always automatically retry delivery of such messages. Depending on the reason of the temporary reject, the message could get accepted at a subsequent delivery attempt. It's always possible to whitelist the sender to disable any checks and to ensure that the message will get accepted as soon as it's retried by the sending server.

### Greylisted

Temporary rejection due to greylisting. This technology is only applied to new IP addresses which do not have a (good) reputation yet in our global systems. We do not apply "classical greylisting" so this should not cause any delays on your legitimate traffic. For new Local Cloud installations please allow up to 72 hours for the systems to "learn" about your traffic.

### Unable to verify destination address

This means the destination server is unreachable or temporarily rejecting the email traffic. You'll have to check the destination route set to ensure delivery is attempted to the correct server. The logs on the destination server should show why it is not accepting the delivery attempts.

### Internal error

An internal error occurred, this should automatically resolve. If not, please contact support.

### Per-minute connection limit exceeded

The sender has exceeded his/her per-minute limit.

### Too Many Connections

Too many connections from the sending server. Rate limited.

### Rejected (5xx SMTP response)

#### **REJECTED**

Messages which have been rejected are blocked by the system. Generally these messages can be reviewed in the "Spam quarantine", from where they can be released. It's always possible to whitelist the sender to disable any checks and to ensure that the message will get accepted as soon as it's resent by the sender.

### Lines in message were longer than user maximum

This means that line within the email is longer than the set maximum. The RFC 5322 (SMTP 5321) specifies a maximum line length of 998. Normal email clients always enforce this limit to avoid delivery problems. The problem should be resolved at the sender side, or the check can be disabled.

### Message had more parts than the user maximum

This refers to the amount of MIME parts a message has. The default limit is set to 100. This can be de-passed and triggered with excessive amounts of attachments or other MIME parts

### Sending server used an invalid greeting

The sender has used an invalid HELO/EHLO. This could be either because an IP address is used for the HELO, or because the HELO contains an invalid character, for example : underscore (\_). The RFC states that a FDQN (Fully Qualified Domain Name) MUST be used.

### Considered spam

Our systems considered this message as SPAM and quarantined the message. Releasing the message from quarantine will report it as a classification mistake to correct our systems.

### SPF failure

This means that the SPF (Sender Policy Framework) has been broken. If this is legitimate mail, then this could be due to a forwarding construction. Please see our SPF knowledgebase article for more information.

### Sending server is missing DNS records

The sending server is missing MX records or A records. Please note that any DNS changes only take effect after the initially set TTL has expired.

### Destination address does not exist

The destination server is rejecting the connection with a 5xx permanent failure. The logs on the destination server will show why the message was rejected. You'll have to resolve the problem on the destination server to ensure it accepts the email.

### Phishing attempt detected

Our systems detected a phishing attempt. Releasing the message from quarantine will report it as a classification mistake to correct our systems.

### Blacklisted sending server

The sending server has been blacklisted on the IP blacklist.

### Sending server listed on multiple DNSBL

The sending server has been found on mutiple blacklists. Releasing the message from quarantine will report it as a classification mistake to correct our systems.

### Sending server attempted too many invalid addresses

The email sending server has attempted to deliver email to too many invalid email addresses in a certain time period. Please retry again later.

### Blacklisted sender

The sender was added to the custom sender blacklist.

### URLBL

A URL within the email has been listed on several blacklists. Releasing the message from quarantine will report it as a classification mistake to correct our systems. The rejection message contains more information about the responsible list.

### External Pattern Match

The layout & format of the email matches known spam emails already listed. Releasing the message from quarantine will report it as a classification mistake to correct our systems. The rejection message contains more information about the responsible list.

### User-specified blackhole address

A user specified a /dev/null Address this email will not get delivered anywhere.

### Combined Score

The "combined" result provides a weighted classification score of the different classifiers. Depending on the configured "quarantine threshold", the message will be rejected as spam or accepted. A quarantine threshold of 0.9 is recommended. To be more tollerable for senders using a wrong HELO/PTR/IP configuration, a score of 0.91 can be set. The lower the quarantine threshold, the more messages will be quarantined as spam. The SMTP message returned for this classification is "High probability of spam" to the sender.

### CRM114

CRM114 is a statistical content check. When a message gets blocked by this classifier on our systems, then this mean there has been a close match within the email that corresponds to an already seen spam message. Releasing the message from quarantine will report it as a classification mistake to correct our systems.

### Tokens

#### Global Tokens

These are statistical content checks that are built based on data collected from all our clusters and clients worldwide. Releasing the message from quarantine will report it as a classification mistake to correct our systems..

#### Cluster Tokens

This is similar to the global tokens, but based specifically on your Local Cloud traffic and

reports.Â Releasing the message from quarantine will report it as a classification mistake to correct our systems.

## Sanesecurity

We make use of certain datasets from Sanesecurity.

## Safebrowsing

In case your message has been rejected with "safebrowsing" in the rejection message, it means it has been (recently) [listed by Google](#) as hosting malicious files.

## Relay not permitted

In case your message has been rejected with "550 Relay not permitted!" in the rejection message, it means that delivery was attempted to the incoming filtering service on port 25 to a domain which has not (yet) been added to the filtering solution. To resolve this, please add the domain to the incoming filtering service. If you're trying to use the outgoing filtering service, please ensure to use the outgoing filtering service port 587 instead.

## Accepted (2xx SMTP response)

### ACCEPTED

Messages that say 'Accepted' have not necessarily been delivered, it means the message has been accepted for delivery. If immediate delivery fails, the message will be automatically retried. If the destination server rejects the email, a bounce will be generated to the sender.Â Reporting the message as spam will correct our systems.

## Message looked like non-spam

This message was accepted for delivery based on our content checks.Â Reporting the message as spam will correct our systems.

## Accepted, DNSWL

The sending server is listed on several DNS-Whitelists. This means no spam has been seen recently from this sending server.Â Reporting the message as spam will correct our systems.

## Accepted, whitelist

The sender has been placed on a manual whitelist by the recipient. Removing the sender/recipient from the whitelist will prevent spam getting through.