

# Scan results explained

Libraesva ESG puts a scan **result badge** when an email in incoming queue is **managed** by the scanning engine.

Some badges can be grouped by colors: each color identifies what message peculiarity caused that scanning result on ESG.

## Rejected

<b>RBL</b>	<b>The message is rejected</b> by ESG because the sender IP address is listed in at least a public RBL
<b>User Unknown</b>	<b>The message is rejected</b> by ESG because the recipient <b>Dynamic Verification</b> test isn't passed
<b>SPF Error</b>	<b>The message is rejected</b> by ESG because the sender IP address isn't allowed to send emails on behalf of the sender domain (envelope from)
<b>Relay Access Denied</b>	<b>The message is rejected</b> by ESG because the sender email server isn't allowed to use the ESG appliance as relay
<b>Invalid Sender</b>	<b>The message is rejected</b> by ESG because the sender address isn't valid, it could be a malformed email address
<b>Helo Problems</b>	<b>The message is rejected</b> by ESG because the HELO procedure failed
<b>Antispoofing</b>	<b>The message is rejected</b> by ESG because is from a sender IP not included in the trusted networks defined in the ESG for the recipient domain
<b>Invalid Sender (DNS)</b>	<b>The message is rejected</b> by ESG because the sender domain doesn't exists or the appliance can't resolve it via DNS
<b>Invalid Recipient (DNS)</b>	<b>The message is rejected</b> by ESG because one or more recipient domain doesn't exist or the appliance can't resolve it via DNS
<b>Sender RevDNS Fail</b>	<b>The message is rejected</b> by ESG because the sender IP address hasn't a PTR record set or the PTR record set doesn't point to the hostname that the server presented with in the HELO process

---

### Message Size

**The message is rejected** by ESG because the sender tried to deliver an oversized message to the appliance

---

### Local RBL

**The message is rejected** by ESG because the sender email server is blacklisted in the the Local RBL service on the appliance. This behavior may be due to a manual RBL blacklist or a dynamic RBL blacklist. The dynamic RBL blacklist happens when an email server sends too many malicious messages. The automatic blacklisting threshold is configurable by the appliance administrator in **Mail Transport → Local RBL → Service Configuration** page

## Clean

---

### Off

**The message hasn't been scanned** by ESG and it's ready for the delivery

---

### Clean

**The message has been scanned** by ESG and it's ready for the delivery

---

### Whitelisted

The from address (or the from/to address combination) matched a whitelist rule. **This message hasn't been scanned** by ESG and it's ready for the delivery

---

### Watermarked

**The message is already scanned** by ESG and returned in the incoming scanning queue. **This badge could be an email loop warning**

## Attachment

---

### Other Infection

**The message is quarantined.** This badge is usually associated to email that had a scanning timeout. The message scanning timeout is a security feature that prevents ESG to be victim of DoS attacks as some malicious messages are conceived to causes the scanner crash.

If this badge is often applied to legit messages, it could be a warning of a undersized appliance: the appliance may need more resources in order to better manage load peaks.

In order to overcome a legit message marked with this badge, you can rescan the message when the appliance load is lower in order to properly perform the scan avoiding false-positive timeouts.

---

Virus infected	One or more antimalware engine on the appliance categorized one or more message attachment as infected. <b>The message is quarantined</b>
Attachment blocked	<b>One or more attachments is blocked</b> by the configured ESG attachment rules
Archive encrypted	<b>One or more archives attached to the message is blocked</b> because of password encryption. All password encrypted archives are not scannable by ESG
Quicksand blocked	<b>One or more attachments is blocked</b> by the Quicksand engine on ESG
Quicksand sanitized	<b>One or more attachments is sanitized</b> by the Quicksand engine (e.g. the active content of the PDF is removed)

---

## Body

---

Whaling	<b>The message is quarantined.</b> The message shows one or more impersonation attempts of a configured Whale name in <b>Content Analysis → Impersonation Protection</b>
Malicious	<b>The message is quarantined.</b> One or more on-board heuristic engine on ESG detected threats inside the message or inside one or more its attachments
Spoofing	<b>The message is quarantined.</b> The message shows one or more impersonation attempts of the sender address or domain
Phishing	<b>The message is quarantined.</b> The message shows one or more attempts of sensitive information or personal data stealing against the email recipient
Spam	<b>The message is quarantined.</b> The message score is greater or equals to the spam value configured in <b>Content Analysis → Anti-Spam Settings → Antispam Action Settings → Spam Levels → Spam Score</b> . The default value is 4.00
High Spam	<b>The message is quarantined.</b> The message score is greater or equals to the spam value configured in <b>Content Analysis → Anti-Spam Settings → Antispam Action Settings → Spam Levels → High Spam Score</b> . The default value is 10.00

---

Blocklisted

The from address (or the from/to address combination) matched a blocklist rule. **This message hasn't been scanned by ESG and has been quarantined**

## Data Loss Prevention (DLP / MCP)

---

MCP Dictionary

The message matched a user defined dictionary rule. **The action performed by ESG depends on the user configuration**

MCP Policy

The message triggered user defined MCP policy rules. **The action performed by ESG depends on the user configuration**

MCP High Policy

The message triggered user defined MCP policy rules and obtained a high MCP score. **The action performed by ESG depends on the user configuration**