# 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

| | |
|---|---|
| RBL | **The message is rejected** by ESG because the sender IP address is listed in at least a public RBL |
| User Unknown | **The message is rejected** by ESG because the recipient **Dynamic Verification** test isn't passed |
| SPF Error | **The message is rejected** by ESG because the sender IP address isn't allowed to send emails on behalf of the sender domain (envelope from) |
| Relay Access Denied | **The message is rejected** by ESG because the sender email server isn't allowed to use the ESG appliance as relay |
| Invalid Sender | **The message is rejected** by ESG because the sender address isn't valid, it could be a malformed email address |
| Helo Problems | **The message is rejected** by ESG because the HELO procedure failed |
| Antispoofing | **The message is rejected** by ESG because is from a sender IP not included in the trusted networks defined in the ESG for the recipient domain |
| Invalid Sender (DNS) | **The message is rejected** by ESG because the sender domain doesn't exists or the appliance can't resolve it via DNS |
| Invalid Recipient (DNS) | **The message is rejected** by ESG because one or more recipient domain doesn't exist or the appliance can't resolve it via DNS |
| Sender RevDNS Fail | **The message is rejected** 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 |
| Welcomelisted | 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.<br>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.<br>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. **The message is quarantined** |
| Attachment blocked | **One or more attachments is blocked** by the configured ESG attachment rules |
| Archive encrypted | **One or more archives attached to the message is blocked** because of password encryption. All password encrypted archives are not scannable by ESG |
| Quicksand blocked | **One or more attachments is blocked** by the Quicksand engine on ESG |
| Quicksand sanitized | **One or more attachments is sanitized** by the Quicksand engine (e.g. the active content of the PDF is removed) |

# Body

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