Virus False Positives

PROBLEM

A message is being tagged as virus, but is clearly a false positive, how can I whitelist sender or avoid such a problem?
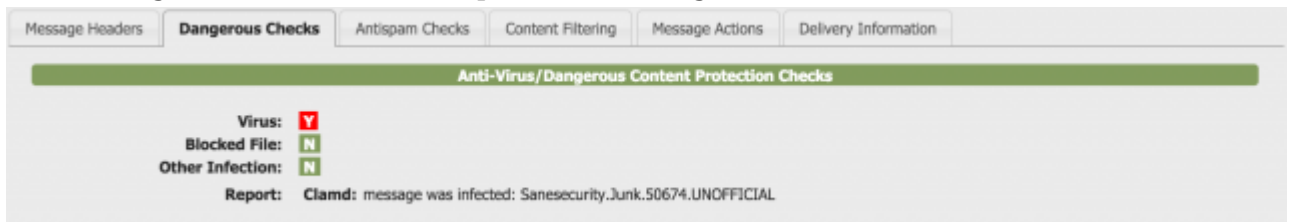
RESOLUTION

Libra Esva does not allow virus senders whitelisting. You can release blocked messages using the **Dangerous Content Release** override function described here:

Dangerous content release override

Correct steps to identify the problem are:

1. Check the **Message Details** report, opening the **Dangerous Checks Tab**, and read the AV engine that is causing the problem. Esva can use up to three AV engines: Clamd, Avira and Bit Defender, plus additional malware and phishing signatures for Clamd by SaneSecurity.

2. If the Dangerous Check detail reports something like:

Message Headers	**Dangerous Checks**	Antispam Checks	Content Filtering	Message Actions	Delivery Information

Anti-Virus/Dangerous Content Protection Checks

Virus: Y
Blocked File: N
Other Infection: N
Report: Clamd: message was infected: Sanesecurity.Junk.50674.UNOFFICIAL

Clamd:message was infected: Sanesecurity.Junk.50674.UNOFFICIAL
that means SaneSecurity Signatures are involved and you may consider changing Libra Esva use of such a feature as these are not real viruses at: ClamAV Antivirus

3. Once identified the AV engine, **submit a False Positive notice** to the vendor, as follows:
   – **Clamd**: http://www.clamav.net/reports/fp
   – **Avira**: https://analysis.avira.com/en/submit
   – **BitDefender**: http://www.bitdefender.com/submit/

×**NOTE:** Libra Esva does not follow up on AV vendors false positive or false negatives.