Blocking Office Macros with Libra Esva

PROBLEM:

How can I block office macros?

SCENARIO 1: Treat Office Macros as Viruses

In the clamav antivirus status page you can enable the “Block Office Macros” option.

This is a system wide setting that will treat documents with office macros as viruses. Emails with attachments containing office macros will be flagged as virus and quarantined. No exception is allowed.

SCENARIO 2: Treat Office Macros as spam

If you disable the “Block Office Macros” option in the clamav antivirus status page, then the office macros will still be detected by the spam filters.

When an office macro is detected, the rule ESVA_OLE2MACRO kicks-in and the spam score of the message is incremented by 5. If you want you can change this score through the spam score override function of Libra Esva.

Exceptions in this scenario can be handled through the whitelists or through custom spam policies.