Sandbox Filters

In this area you can configure the available sandboxes: QuickSand and UrlSand.

The sandbox configurations can be customized on a domain basis, which means that you can have the same settings for all the domains hosted on ESG or you can have different options for some of them

UrlSand Defense

This is an URL sandbox.

When the option “Enable URI Sandbox” is enabled, the URLs present in the email are rewritten so that when the user clicks on it, the browser lands on our cloud sandbox.

The cloud sandbox analyzes the URL in real time and redirects the user to the page of the original link unless it is suspicious or plain dangerous.

All the details on how it works and how to whitelist domains (so that the urls pointing to those domains are not rewritten) in our knowledge base article.

The option **“Automatically create URLSand links in Html text”** rewrite all non href links to an HTML text (eg. www.contoso.com instead of href=”www.contoso.com”)

The option “**Do not allow users to skip URI Sandbox checks**” disable the possibility to go to the original link even if the sandbox identifies it as dangerous.

When the option “**Show preview for suspicious pages**” is selected, in case of a suspicious page is requested, the URLSand returns the screenshot of the page, asking confirmation to

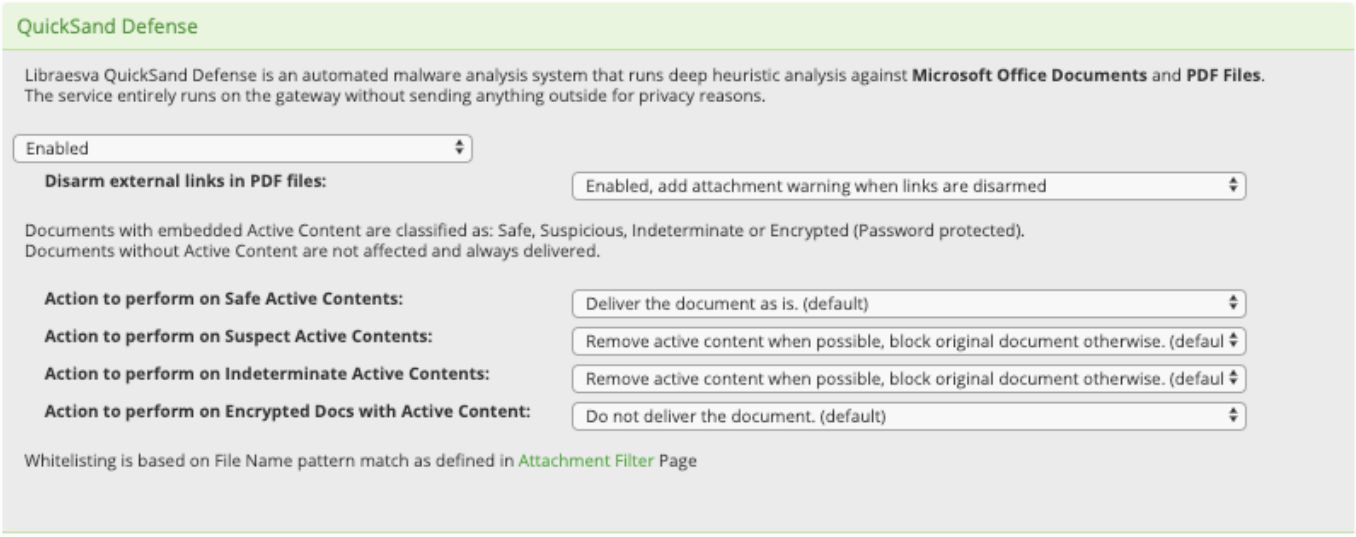
visit it.

You can also avoid a specific link to be rewritten using Phishing Safe section.

QuickSand Defense

This is a File sandbox for documents (Microsoft Office documents and PDF documents).

The file sandbox **runs on the gateway**, which means that your files never leave ESG.



As the name suggests, this is a very quick sandbox, it does not introduce delays and is not vulnerable to sandbox escape techniques. The files are analyzed during the email analysis and if they contain active content (macros, embedded executables, javascript code) the active content is analyzed and classified.

Possible classifications are: safe, suspicious, indeterminate, encrypted (encrypted active content cannot be investigated). For each of these categories you can choose an action: deliver the file, sanitize and deliver (the active content of the document is disarmed), block (the file is removed from the email).

There is a specific option related to PDF files. Libraesva ESG QuickSand is able to disarm links inside PDFs. When doing so, you can choose to add a text file to the email explaining that the sandbox disarmed the links or not to add the warning text file. The disarmed PDF file is always delivered.

×**NOTE** Quicksand, like the antivirus, is not influenced by the whitelist for security reasons. To bypass the scanning for some files from trusted sources, you can create a “File name rule” from “System -> Content Analysis -> Attachment Filters”

Additional details in the knowledge base article.