How the Libra ESVA QuickSand file sandbox works

What is the Libra ESVA QuickSand file sandbox

It is a service that protects from malicious active content in Microsoft Office and PDF files.

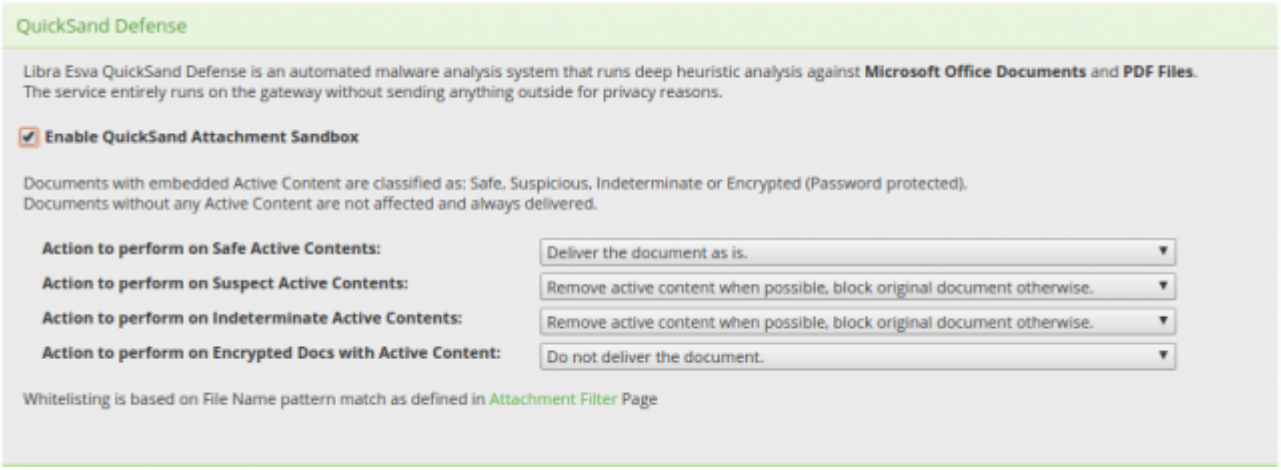
Active content is any executable code embedded in the document like macros, javascript code, ActiveX applications.

The **QuickSand** sandbox **runs on the gateway**, which means that the files never leave ESVA.

As the name suggests, it is a very quick sandbox: the attachments are analyzed in the same pipeline of the email analysis without additional delays, it is not vulnerable to the sandbox evasion techniques.

The **QuickSand** sandbox identifies active content inside documents and classifies it based on the behavior. The possible categories are:

- **safe**: active content is present and it does not perform any critical operation in respect to security
- **suspicious**: potentially critical actions are performed by the active content like downloading data from the internet, launching programs, performing actions on the filesystem and so on
- **indeterminate**: active content is present but for technical reasons it’s behavior cannot be categorized with sufficient accuracy
- **encrypted**: the document is encrypted and therefore it is not possible to tell whether there is active content inside



For each of these categories, you can choose what to do with the file:

- **deliver**: deliver the file as is
- **sanitize and deliver**: disarm the active content and deliver the disarmed document
- **block**: do not deliver the file, it will be removed from the email

Not all of these actions are available for all the the categories, for safety reasons. You can also define fallback actions in case the document cannot be sanitized for technical reasons. In this case you can either fallback to deliver or block.

The default actions are what we suggest as the best compromise.

The attached documents are analyzed and cleaned/removed also if they are contained in archives, even if the archives are nested inside other archives.

When a file is either sanitized or blocked, the entire email message is quarantined so that the original version of the file remains available for a release should it be needed.