Mail Encryption module

Its goal

Libraesva ESG Mail Encryption is an **End-to-End** encryption feature that protects your emails directly on the gateway. End-to-End encryption ensures that **only the intended recipient can read the content**. Not even administrators can read the message without the password.
This is the same encryption approach that Whatsapp uses.
The **encryption** is done **after the content analysis**, so the whole Libraesva ESG protection is applied to the message and **security is granted** as always.

How it works

The appliance administrator defines **Encryption Policies** that are basically regular expressions run against the email subject. When the subject matches the regular expression set, the message is **encrypted** by the appliance. Libraesva ESG encrypts the message **body** and optionally the **subject**.

When the message has been encrypted, a password to decrypt it is **generated** by the ESG. This password is, by default, automatically sent to the sender of the message.
It's the **responsibility** of the sender to communicate the password to the intended recipient(s).

Note: the only way to make sure the message is secure, is to send the password using a different communication channel like SMS, WhatsApp, voice call and so on, but **you should not send the password by email**.

Since the password generation, all new messages to that recipient(s) will be encrypted with the same password.

If the sender loose the password, the password can be reminded to him from the Mail Encryption page.
If the sender suspects the password has been stolen by someone, he can revoke it from the Mail Encryption page.

To learn more how to set up this module, please read the Mail Encryption manual.