Encryption at rest

Encryption at rest is available in Libraesva ESG since version 5.3.

Functionality

Libraesva ESG email quarantine is now encrypted in order to protect the data at rest.

The feature is completely transparent to the administrators and to the users, no action is required during the initial installation or at the reboot of the appliance.

After an upgrade from Libraesva ESG 5.2 to Libraesva ESG 5.3 the previous quarantine, which was stored unencrypted, is automatically encrypted in the background. The new messages that are received after the upgrade are encrypted before being stored.

Implementation

The “encryption at rest” feature has been implemented by balancing the need to protect personal data at rest with the fundamental requisite of high resilience and reliability of Libraesva ESG.

The high-entropy encryption key is unique for each appliance, it is generated during the first setup and it is stored in a protected vault separately from the encrypted data.