Basic configuration and settings for the encryption service

This guide provides a configuration and implementation overview of EveryCloud's Encryption service

1.1 Activating encryption

Login in to your control panel using the Administrators account credentials. Then navigate to your primary domain and select the Management - Email - Encryption tab.

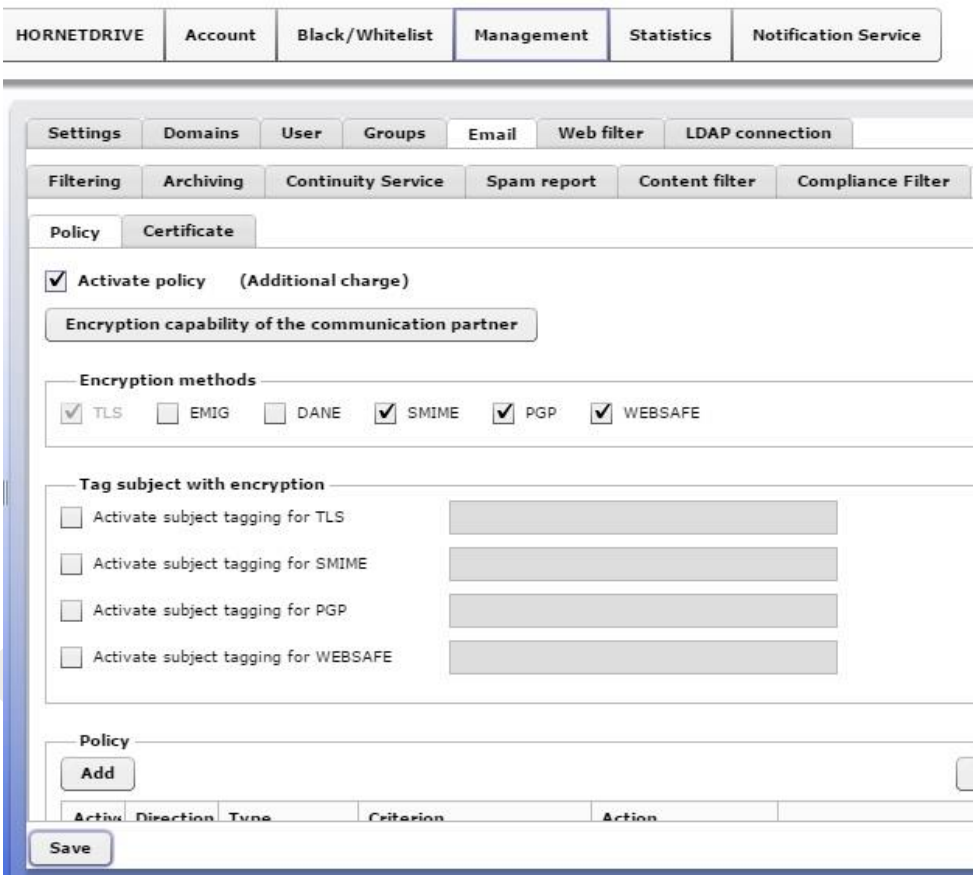

Figure 1: Encryption menu

To be able to use the encryption service, activate the tick at "Activate policy" as shown in Figure 1.

1.2 Verify the encryption capability for a communication partner/recipient

You can verify the encryption capability even before any further configuration of the encryption guidelines is carried out. Enter the email addresses one after another using the syntax shown in Figure 2 and confirm by clicking on “Verify

Figure 2: Verify encryption capability

As soon as the verification of the addresses entered has begun by clicking on “Check”, the address/addresses will be checked for encryption compatibility. (see Figure 3) depicts the recipient’s encryption compatibility.

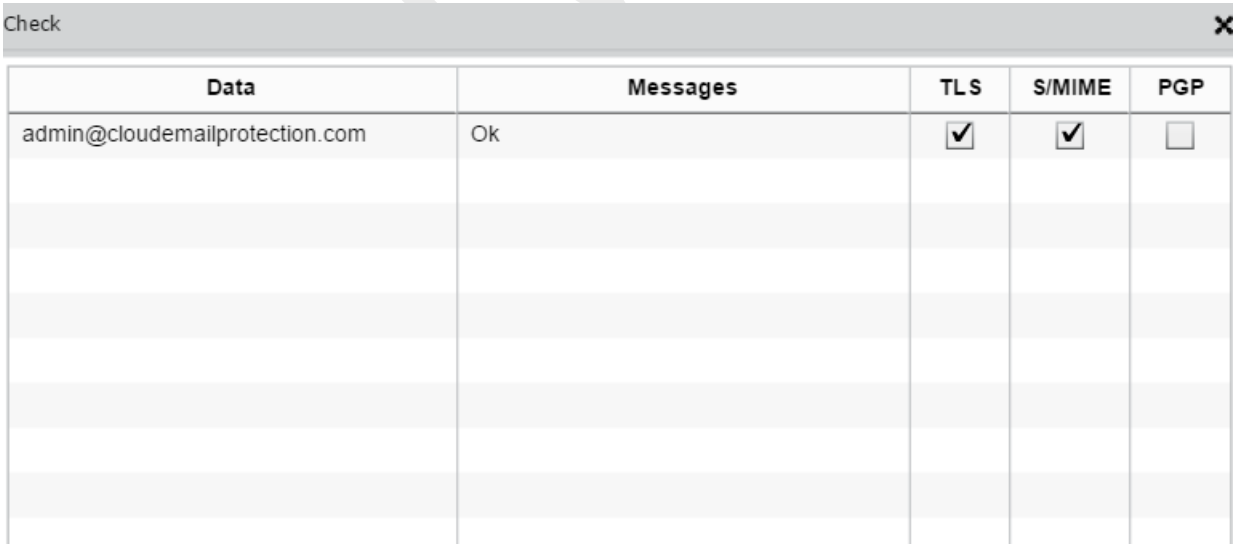

Figure 3: Verify encryption capability

1.3 Set global communication guidelines

TLS encryption, can either be set as mandatory or opportunistic.

Mandatory means the connection must be forced via TLS, whereas opportunistic means where possible. Encryption of an entire domain by S/MIME or PGP can only be set as “where possible” or deactivated. (S/MIME or PGP encryption can be forced for individual email addresses. In this connection see the following section, 1.4.

If a policy is set as mandatory the email will not be sent if a secure TLS connection cannot be established. The sender will then receive an appropriate error message.

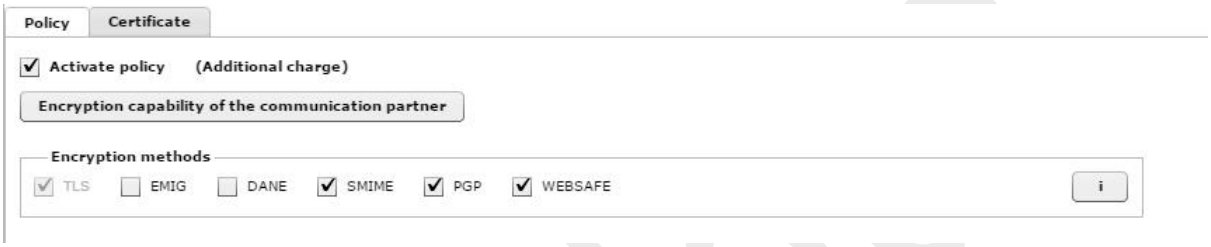

Figure 4: Global encryption settings (domain level)

1.4 Set deviating communication guidelines

Global policy exceptions for individual senders or recipients can be configured using the ‘Add’ button.

It is also possible to force S/MIME or PGP encrypted transmissions by using this function if the recipient supports SMIME and PGP

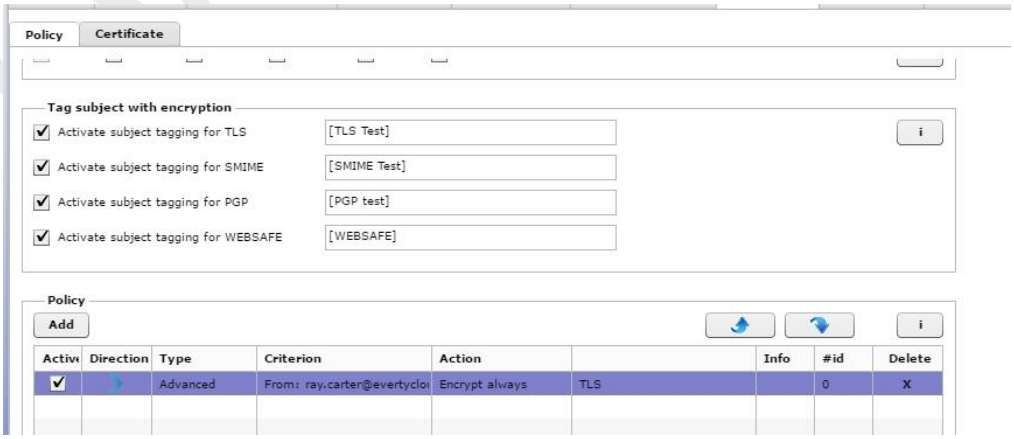

Figure 5: Define exceptions (domain & user levels)

2. Certificate administration

You will find the certificate administration in the “Certificates” area. There, the certificates for your domain users can be entered and ordered.

Figure 6: Certificate order

2.1 Order for certificates

The certificates required for encryption can be ordered directly via the control panel. For this purpose, change to the “Certificates” tab. Select one of the proposed users and enter the first and second names exactly (see Figure 6). Please check your entries before you confirm and store them by clicking on “Order” because, as a digital signature, the certificate is only valid with the correct name. After storing, a binding order for the certificates is placed.

3. Use of the Websafe encryption service

The Websafe encryption service can be activated and used for the respective communication partner where under “Deviating communications guidelines” an email address has been set, the option, “Websafe” has been selected and none of the other selected encryption methods can be used.

In order to encrypt an email safely by Websafe without such deviating communications setting, enter the keyword, “WEBSAFE” or “CRYPT” specifically in the subject line of your email (see Figure 7). Upon transmission, the email will then be encrypted by EveryCloud.

Figure 7: Sending an email via Websafe

If an email cannot be sent to the recipient in an encrypted form due to a missing certificate, the email will be forwarded to the EveryCloud Websafe instead and will be stored there.

The email recipient will then receive a separate informative email with the access data to his personal Websafe. A first time PIN for activating the Websafe will be sent in parallel to the sender, who must forward this PIN separately to the recipient. Email and PIN together provide the recipient with access to his Websafe. There, he can set his personal password and view the encrypted message.

Meaning of the keywords for using the Websafe:

By using the keyword, “CRYPT”, the following encryptions methods are used in order:
S/MIME, PGP, TLS, Websafe.

By using the keyword, “WEBSAFE”, the following encryption methods are used in order:

S/MIME, PGP, Websafe (no TLS).

Please note that keywords must always be written in capital letters to use the Websafe.

Note: Websafe access is enabled for one user and remains available to be used for future Websafe messages.