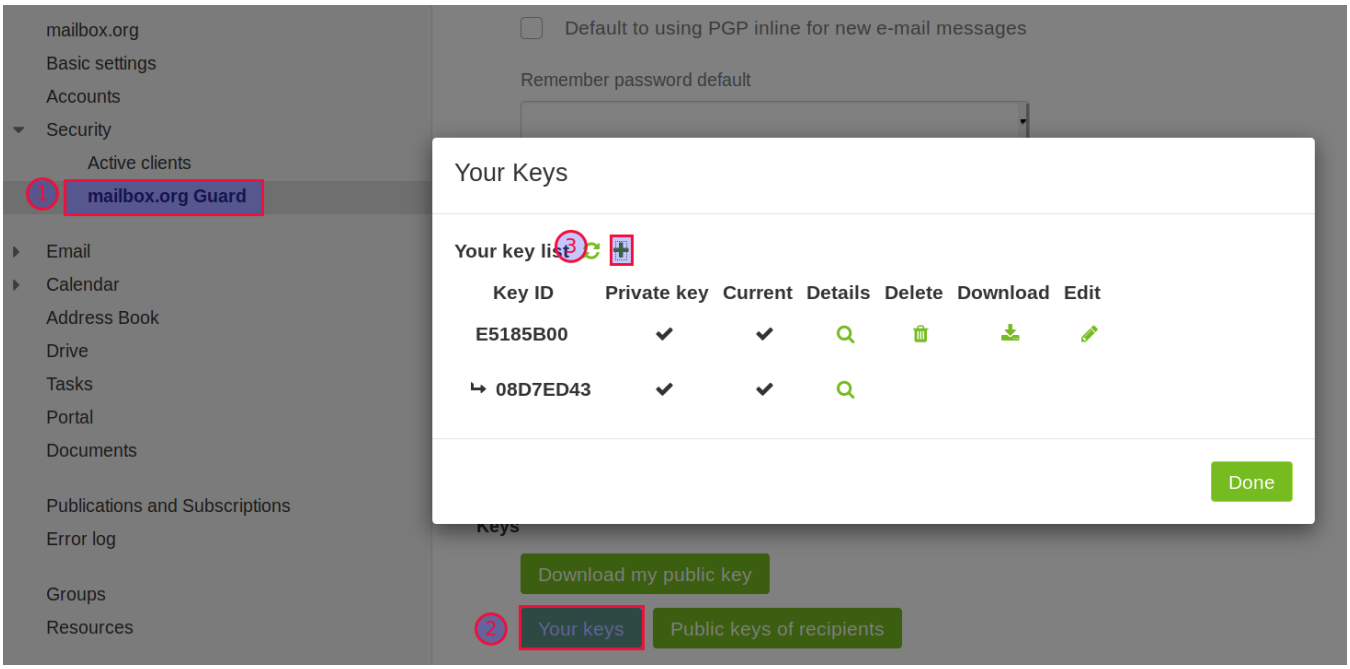
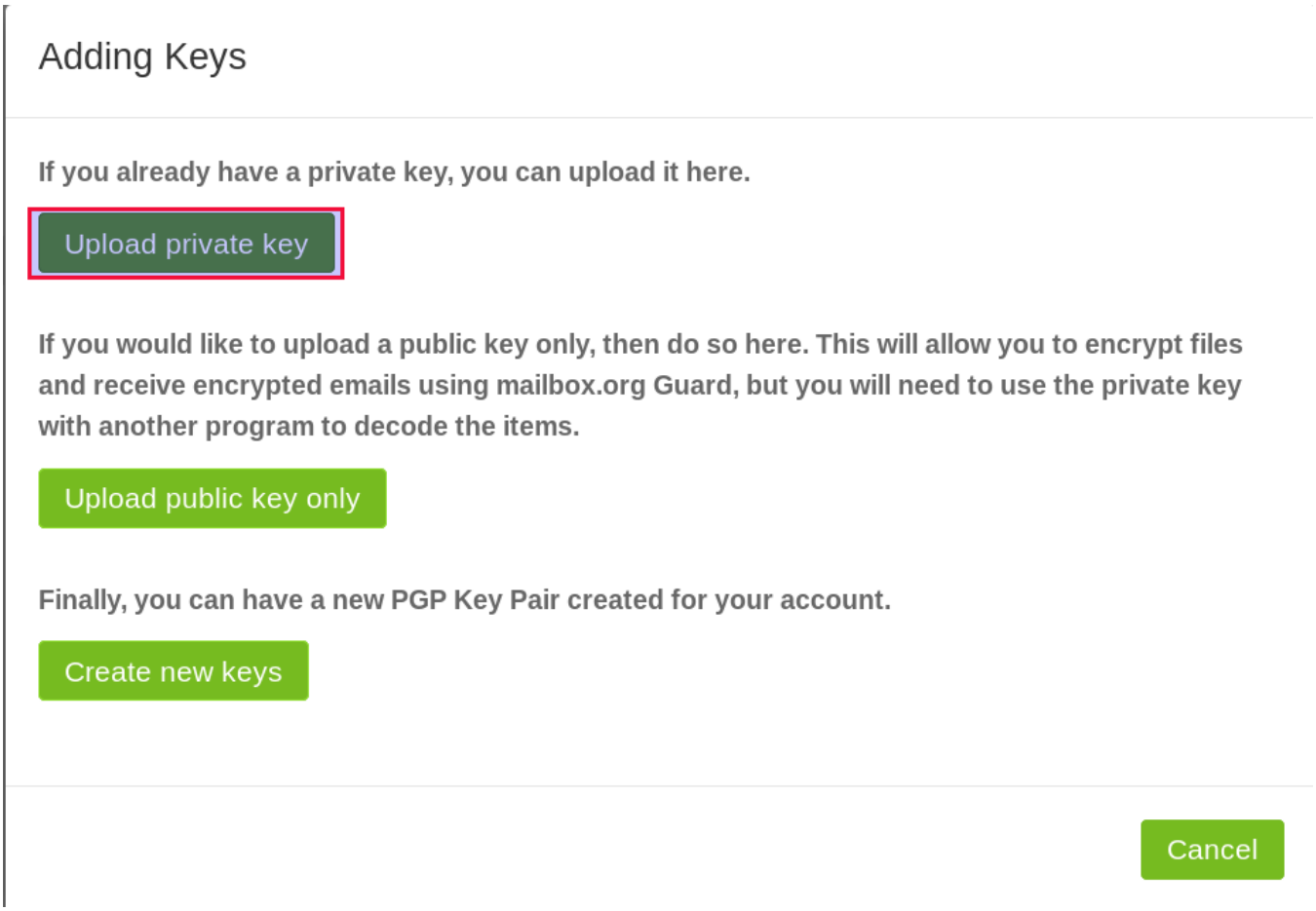
Import existing PGP keys into Guard

You may replace the automatically created PGP keys on our server with your own. Note that any custom keys need to state your primary mailbox.org e-mail address as UID.

First, open the Guard PGP key management and upload your new key to the server. In order to upload a new key, click on the “+” symbol in your key list.



Now the following dialog appears. Upload your private key.



Once the upload is finished, you can delete the (old) default keys that were previously generated by the Guard.

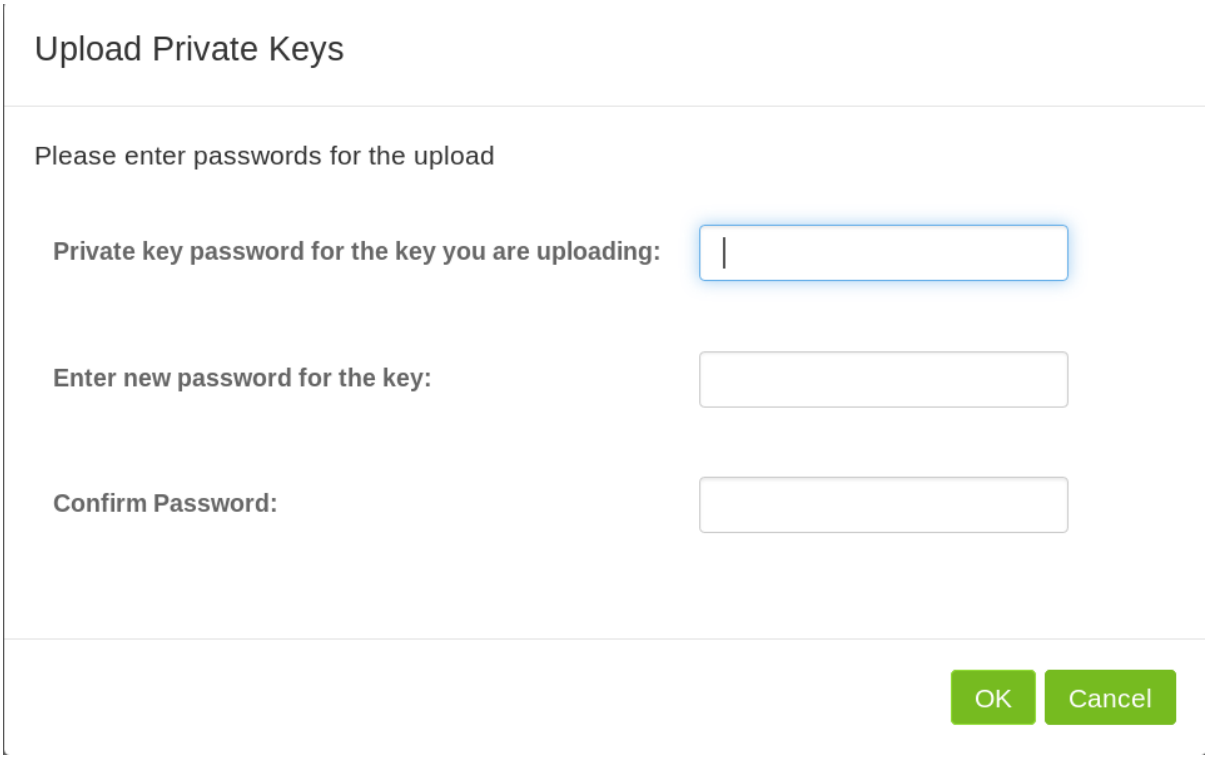
Users with critical security requirements should consider not uploading their private PGP key to our server but only the public key. It is possible to just provide the public part of the key so that other Guard users can encrypt any messages they wish to send to you. However, without the private key it won't be possible to read Open-PGP-encrypted e-mail via Webmail in the browser. Of course, you can still access these e-mails with any mail client that has the necessary local PGP configuration in place.

If you upload a private PGP key, or a pair of private and public keys, you will be asked to enter two passwords:

1. The existing pass phrase that you chose to secure your private key on the local computer. This will be required to decrypt the key for upload.
2. Enter a new password

   > Important: Please do make sure you enter the same password as your existing Guard password.

   This is required to control access to the private key stored in mailbox.org Guard.
   If you fail to enter a password that is identical to your existing Guard password, then you will lose access to any previously created keys – which means you won't be able to delete them.



Once uploaded, the new keys will be flagged „current" and the previously used keys become inactive. You can now delete the inactive keys by clicking on the related trash bin symbol. Note that you will be asked to enter the Guard password when trying to delete a private key.

Beware: Only delete old keys if you are absolutely certain that you will not need them anymore. If there are still e-mails or files stored in your account that were previously encrypted with the old key, you will no longer be able to decrypt and read these after you've deleted that key.

Note: Because of a bug it is not possible to directly upload the public keys generated by OpenPGP smartcards (e.g. Nitrokey, Yubikey 5) to mailbox.org Guard. A workaround is available – please contact support.

Related Articles

- Which PGP standards are supported
- The Encrypted Mailbox
- Can I trust the staff at mailbox.org
- How to set up Mailvelope
- PGP key management