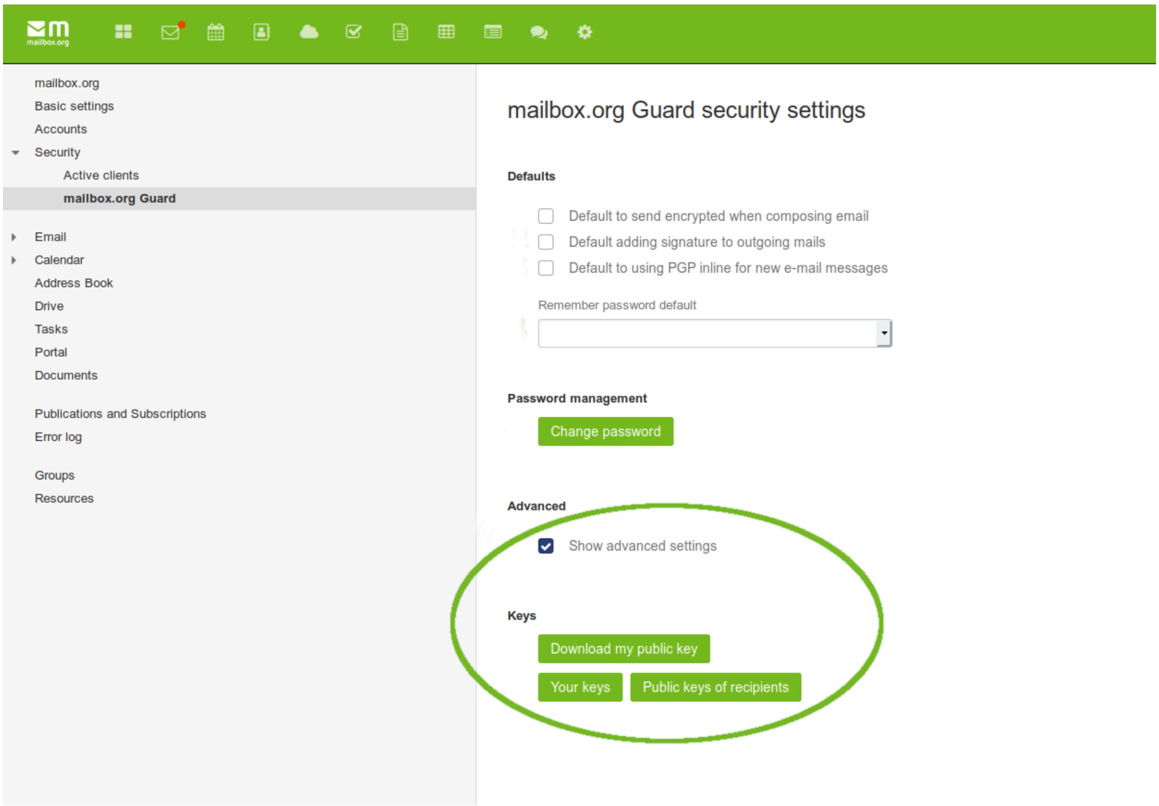
PGP key management

Note: to use the features described in this article, you must have the mailbox.org Guard enabled.

Note: The mailbox.org Guard is designed to work with your main email address. **It is not intended to be used in combination with aliases.**

The mailbox.org Guard provides an administration for your own PGP keys and the public PGP keys of your communication partners. You can find this administration in your mailbox.org office under "**Settings -> mailbox.org Guard Security**":



mailbox.org Guard security settings

Defaults

□ Default to send encrypted when composing email

□ Default adding signature to outgoing mails

□ Default to using PGP inline for new e-mail messages

Remember password default

Password management

Advanced

☑ Show advanced settings

Keys

Once mailbox.org Guard is enabled, two pairs of keys will be created. The keys are then used automatically by the software such that users do not normally need to concern themselves with them.

1. The master key (first key pair) will be used to sign emails. It can be used for certification of other keys too (web of trust), but this feature is not implemented in mailbox.org Guard.
2. The secondary key will be used for encryption and decryption of emails and files in drive.

The PGP keys which have been generated on our server can be downloaded from the key management section. This is useful if you have a local PGP installation on your PC or mobile phone, and would like to set up a mail client on these devices that uses the same keys. This will enable parallel access to your encrypted e-mail both via Webmail and by your local e-mail programs.

Please note: The mailbox.org Guard has been designed to work with your account's main e-mail address. Using it in combination with e-mail aliases is not supported.

Import your own, existing PGP keys

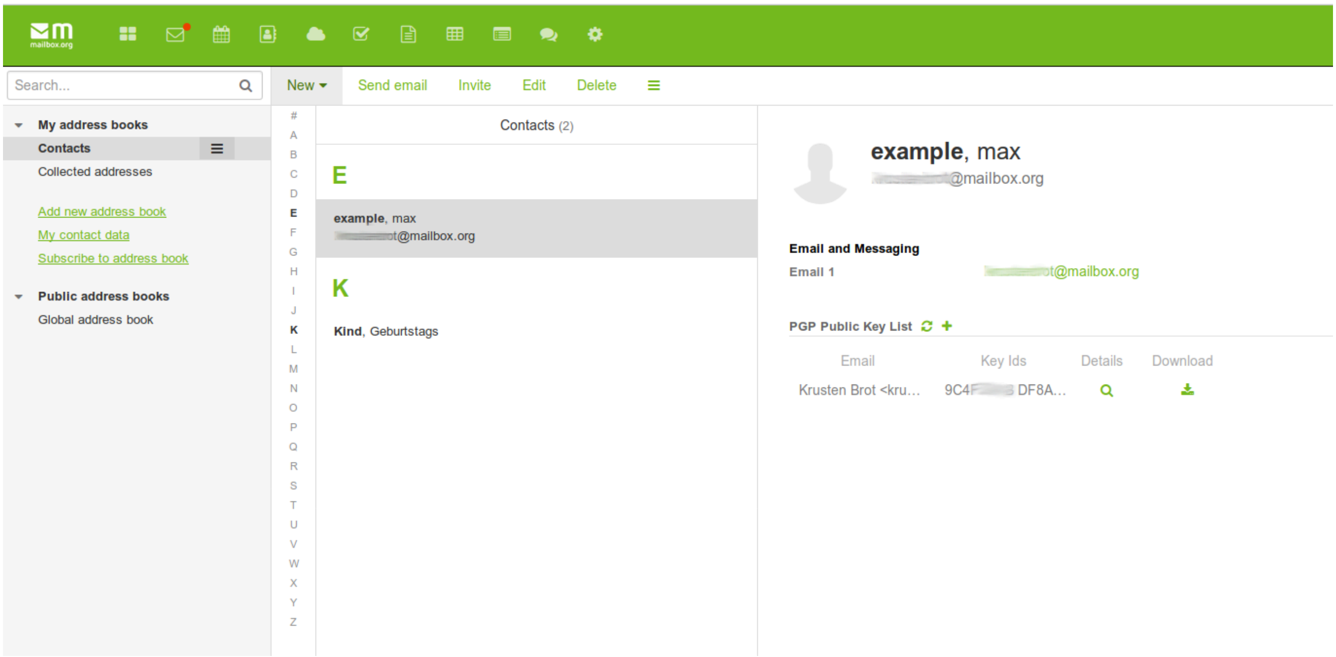
You may replace the automatically created PGP keys on our server with your own. Note that any custom keys need to state your primary mailbox.org e-mail address as UID. Users with critical security requirements should consider not uploading their private PGP key to our server but only the public key.

Please note: You must have a valid private key in place on the server in order to be able to read encrypted e-mails in the browser or open encrypted files on the Drive.

Public keys of communication partners

You may add the public keys you got from your communication partners here to. Click on the "+" symbol in the public keys section to upload a public key.

Additional you may manage the public keys of you communication partners with the addressbook. Open the addressbook entry. You can upload a public key with a click on the "+" symbol in the public keys list.



example, max
[redacted]t@mailbox.org

Kind, Geburtstags

example, max
[redacted]@mailbox.org

Email and Messaging

Email 1 [redacted]t@mailbox.org

PGP Public Key List

Email	Key Ids	Details	Download
Krusten Brot <kru…	9C4F[redacted]DF8A…	🔍	⬇

Supported maximum size of key files

Note: The file size of any public PGP keys uploaded to mailbox.org must not exceed 65 kilobytes, which is sufficient for most keys. However, if a key contains image data or very many signatures, the file may be larger, and this will likely cause upload problems.
To reduce the file size of an over-sized key, open the file locally with the GnuPG key management tool and export a leaner version as follows:

```
> gpg --armor --export-options export-minimal --export <yourKeyID> > yourFileName.asc
```

If you don"t have GnuPG available locally to export the key like this, please ask your communication partner to provide a smaller key file.

Related Articles

- An introduction to mailbox.org Guard
- Import existing PGP keys into Guard
- Is there going to be transport encryption for my e-mail
- Setup Gpg4win for Windows
- HowTo: YubiKey NEO as PGP smartcard