How to set up Mailvelope

Users can install the browser add-on Mailvelope in Mozilla Firefox or Google Chrome and then use it with the mailbox.org Office. Doing so has a number of advantages:

- Mailvelope can work in concert with the OpenPGP e-mail encryption features of the mailbox.org web interface. That means e-mails can be encrypted, descrypted, and signed easily.
- OpenPGP key management on the local computer.
- Distribution of your public OpenPGP key to other communication partners via mailbox.org Guard or through our dedicated HKPS key server.
- Secure transmission of your private key to different devices via the mailbox.org Office is possible.

At the same time, we need to point out some of the risks that come with using the Mailvelope add-on. Please take note of the following **security warnings**:

- Your keys will be saved in the browser storage on the client computer, which is potentially unsafe. The OWASP's HTML5 Security Cheat Sheet recommends NOT to save any security-sensitive information in the browser's Local Storage, as the data stored there is vulnerable to cross-site-scripting (XSS) attacks. This Security Analysis of Mailvelope (PDF) also points out the fundamental risk of XSS attacks that Mailvelope is subject to. Users of the popular Mozilla Firefox are particularly affected, because this browser offers less protection features than, say, Google Chrome. For this reason, we recommend users of Firefox who wish to use the **Mailvelope add-on to do so only in combination with the NoScript add-on enabled**. NoScript contains a number of security features that are missing in plain Firefox, including protection against cross-site-scripting.
- Javascript was never designed to be used as a programming language for crypt-applications. Some cryptographic security mechanisms that are considered best practice cannot be implemented in Javascript due to the limitations imposed by its sandbox runtime environment. For instance, it is not possible to remove a private key from main memory after it has been used because Javascript has no access whatsoever to the operating system's memory management functions (Overwriting memory - why?). Note that the way Mailvelope works has been considered a security bug by Tor Onion Router (german).

Our perspective is that while Mailvelope is certainly easy to use and does the job, it is unfortunately not suitable a tool for secure environments.

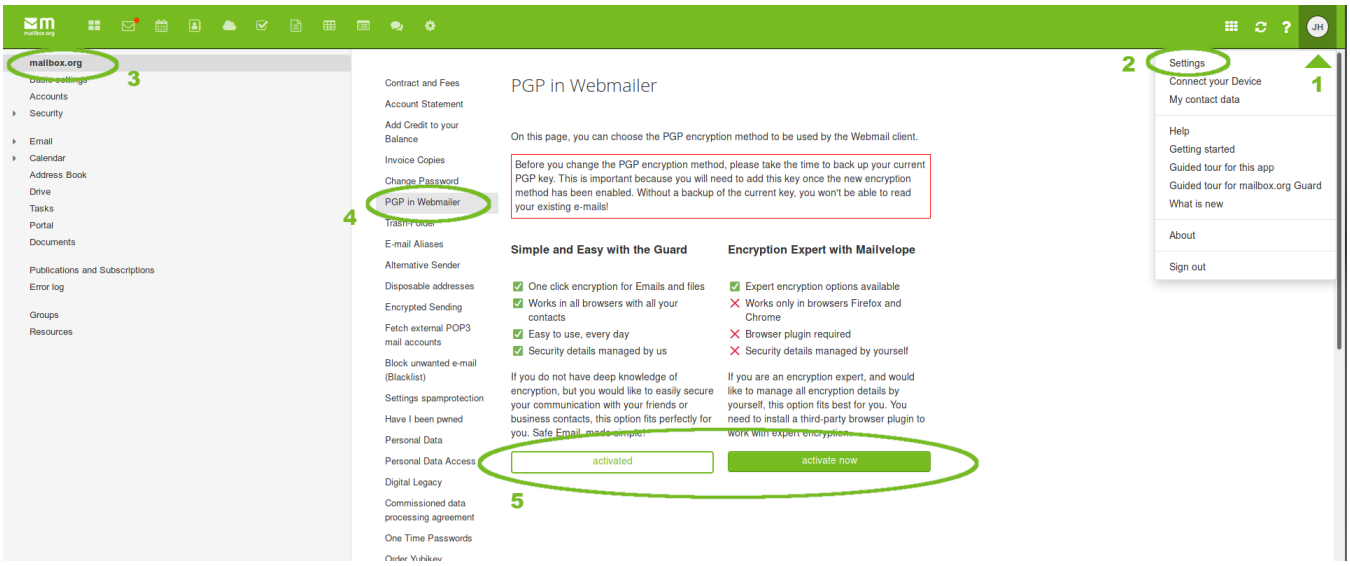
- The major disadvantages of all browser plug-in solutions thus far are that they cannot properly deal with attachments saved in cloud storage, and cannot be safely used in Internet cafes or with other third-party computers (like PCs in Hotel lobbies, etc.)

Installing Mailvelope

To use Mailvelope with the mailbox.org Office, simply install the add-on in your browser. Users of Mozilla Firefox should make sure to also install the NoScript add-on for improved security. The latest version of Mailvelope has been pre-configured to work with mailbox.org without requiring any further configuration steps.

Enabling Mailvelope Support

After completing the Mailvelope add-on configuration, log in to mailbox.org and go to **Settings - mailbox.org - PGP in Webmailer** to set up and activate the mailbox.org Guard and OpenPGP encryption. When asked to select a security solution pick the option Mailvelope. Weh done, configure the Add-On itself.



Related Articles

- Move away from Gmail to mailbox.org - step-by-step
- How to use two-factor authentication - 2FA

- Setup with K-9 Mail for Android
- Setup with Mail.app for iOS
- How to set up team accounts