Two-Factor Authentication

So far three methods for *Two-Factor Authentication* are implemented: U2F, Yubi OTP, and TOTP

- For U2F to work, you need an encrypted connection to the server (HTTPS) as well as a FIDO security key.
- Both U2F and Yubi OTP work well with the fantastic Yubikey.
- While Yubi OTP needs an active internet connection and an API ID + key, U2F will work with any FIDO U2F USB key out of the box, but can only be used when openemail is accessed over HTTPS.
- U2F and Yubi OTP support multiple keys per user.
- As the third TFA method openemail uses TOTP: time-based one-time passwords. Those passwords can be generated with apps like "Google Authenticator" after initially scanning a QR code or entering the given secret manually.

As administrator you are able to temporary disable a domain administrators TFA login until they successfully logged in.

The key used to login will be displayed in green, while other keys remain grey.

Yubi OTP

The Yubi API ID and Key will be checked against the Yubico Cloud API. When setting up TFA you will be asked for your personal API account for this key. The API ID, API key and the first 12 characters (your YubiKeys ID in modhex) are stored in the MySQL table as secret.

U2F

Only Google Chrome (+derivatives) and Opera support U2F authentication to this day natively. For Firefox you will need to install the "U2F Support Add-on" as provided on mozilla.org.

U2F works without an internet connection.

TOTP

The best known TFA method mostly used with a smartphone.