How to use two-factor authentication - 2FA

mailbox.org offers everyone the option to use **Two-Factor Authentication („2FA“)**.

With 2FA, your previous account password will be replaced with a new pass phrase that combines two different components (the “factors”). The pass phrase is made up from one factor that represents „something you know” - a **PIN** - plus another factor that is “something you have” – such as a hardware token or software program on a hardware device that can generate a special **One-Time-Password** (OTP) for single use.

There are different methods available for implementing 2FA. We will briefly describe how they work and what the key differences are. We will also show you how to configure these methods for use with your account.

We understand that some of our customers may need detailed guidance, while others are power users with significant IT experience. No matter how experienced you are, we kindly ask you to read this article carefully, especially the information under section 4.

Contents:

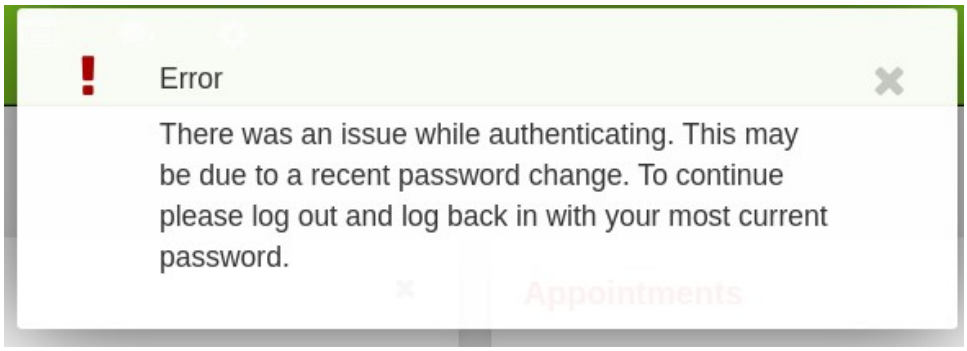
Our 2FA implementation offers protection in the following scenario:
You would like to log on to our service using a device that is not secure and potentially unsafe to use. It’s a judgment for the user to make but as a general rule, any device that may have been compromised by viruses, trojan software, etc. without your knowledge should be considered not secure. For most people, the following examples would fall under the classification of “not secure”:

- Publicly accessible devices such as those in Internet cafés
- Computer terminals in hotels
- Devices of friends and associates

You can safely log on to our services on such devices using two-factor authentication. By combining a **PIN** with a **one-time password**, your existing account password remains protected. The account password is normally that which you originally created when registering with mailbox.org.

If you decide to use 2FA with your account, then this will also come with a few **restrictions:**

- You cannot change your **main e-mail address** as long as any of the two available OTP security levels are enabled for your account.
  If you do need to change your main e-mail address, go to **Settings (click on the cogwheel symbol in the upper right area) mailbox.org One Time Passwords**.
  Set the option **OTP security level** to **Off, just normal passwords**. Then change the main address with which you normally log in.
  You can then subsequently set the OTP security level back to its previous value.
- You cannot log on to the mailbox.org Office using **several clients (browser windows, or devices) at the same time**. Only a single authenticated session is permitted when using two-factor authentication.
- **You must log off before closing the browser window to end your session**. Make it a habit to do this, even if you don’t use OTPs.
  If you forget to log off, you will see an error message the next time you’re trying to log on.



  If you encounter this error message, then please log off.
  To log off properly, click on the circular avatar icon in the upper right corner of the browser window and then click **Sign out**.
- If you set the OTP security level to **Web service OTP, other Services off**, then it will no longer be possible for you to log in to our help desk or the user forum!
  As a workaround, you can post in the forum using a newly registered test account.
  It will be possible to communicate with the helpdesk through an e-mail address you have previously specified at https://help.mailbox.org
- **Two-factor authentication can only be enabled for logins to the web-based client**. All other services such as IMAP, POP3 and SMTP that use a **local e-mail client or data synchronization** via WebDAV, CalDAV, and CardDAV (and the corresponding clients) **are not supported to use 2FA**.

This functionality is also supported for those who use mailbox.org with their own domain name.

We offer two ways of accessing **two-factor authentication („2FA“)** for your mailbox.org account. These differ with respect to the “something-you-have” element that we mentioned at the beginning of this article:

- **Hardware token**:

A hardware token offers somewhat **better security than** the so-called **"soft" two-factor authentication** that uses another device & software, like a smartphone app, for example.
The following hardware tokens are supported:

a. **mailbox.org YubiKey**:
We think the best option is to use a YubiKey from mailbox.org. These YubiKeys are authenticated against a YubiKey server that we operate in our data center. This means the transmitted data does not need to be synchronized with the YubiCloud.
Information about the range of YubiKeys that are available through us can be found in this article. Further details on how to register your YubiKey with the YubiCloud in order to use it in connection with other web services are provided in this article.
b. **Third-party YubiKey**:
You can also purchase a Yubico-made YubiKey from other vendors. In this case, authentication is performed through the world-wide YubiCloud.
c. HOTP- or TOTP-compatible **tokens** such as Nitrokey Pro or **Nitrokey Storage**.

- **Software token**

Software tokens are sometimes also called **"soft" 2FA** or **OTP generators**:
You can use OATH-, TOTP-, HOTP-, or mOTP-compatible tokens. These will be installed on a smartphone, through apps such as **FreeOTP**, **Google Authenticator**, or the **OATH Token App** for the iPhone.
Please make yourself aware of the security-related disadvantages of software tokens before opting for this method. Make sure your software token generator originates from a trustworthy source such as F-Droid and is maintained properly.

We do not offer SMS-based 2FA and do not intend to in the future, either, as this authentication method is not considered secure and therefore not recommended.

Important note: If you have 2FA enabled on your account and then lose your YubiKey or the device that you use to generate software tokens with, then the only way to reset your password is through one of the authorized password reset methods for your account - these need to be set up beforehand.

Unfortunately, we cannot offer support for any YubiKeys not bought directly from us.

Access the settings page in your mailbox.org-Office by clicking on the **cogwheel symbol in the upper right corner of the window mailbox.org One Time Passwords**:

a. Specify a four-digit **PIN**.
The PIN may contain uppercase and lowercase letters as well as numbers, but not any special characters. If you enter more than four characters, any excess characters will be trimmed off and ignored.
Make a note of this PIN and keep it secure, either physically in a safe place, or by using a password safe application such as KeepassXC.

Make sure that both PIN fields contain the PIN before you continue.

b. Specify the desired **security level**.

We offer two different security levels for our two-factor authentication:

- **Web service OTP, other Services password:** This is the most common level for two-factor authentication at mailbox.org, and similar to how the majority of e-mail providers handle 2FA. You log in to the web interface using a PIN and a one-time password. However, all other services such as IMAP, POP3, SMTP, WebDAV, CalDAV, CardDAV or ActiveSync will not use 2FA and require your (normal) password to be entered. You can continue to use local e-mail clients on your PC or smartphone, synchronize calendars with other devices, and so on.
- **Web service OTP, other Services off:** This is a security level for special use cases that is only available at mailbox.org. After choosing this option, you will only be able to log in to the web client at https://www.mailbox.org using a PIN and a one-time password. All other services will be disabled for your account. This also means that you cannot use local e-mail clients or synchronize any data with mailbox.org.

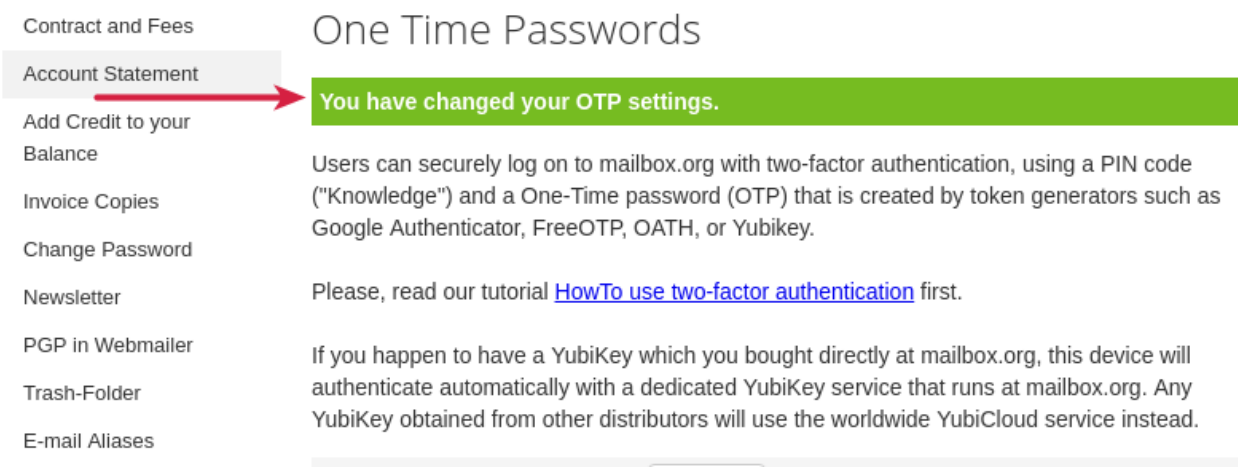
c. Now select the OTP method: **mailbox.org YubiKey**

d. Insert the Yubikey into a free USB port on your computer and use your mouse to left-click into the empty form field that is situated next to **OTP password test**.
On the YubiKey, press once the golden button that has the **Y symbol**. A code will now be generated automatically and inserted into the form field that you just clicked on.

e. **In the web interface**, click on the green button hat says **Perform OTP Passwort test**.

f. If the test was successful, click the button **Save**.

Please note the success message at the top of the page:



Finally, log out to finish the setup.

Your two-factor authentication is now active. From now on, you will log in with your PIN in combination with the Yubikey's one-time password.

If the test has not been successful, please repeat the token setup.

- Access the settings page in your mailbox.org-Office by clicking on the **cogwheel symbol in the upper right corner of the window mailbox.org One Time Passwords**:

a. Specify a four-digit **PIN**.
The PIN may contain uppercase and lowercase letters as well as numbers, but not any special characters. If you enter more than four characters, any excess characters will be trimmed and ignored.
Make a note of this PIN and keep it secure, either physically in a safe place, or by using a password safe application such as KeepassXC.

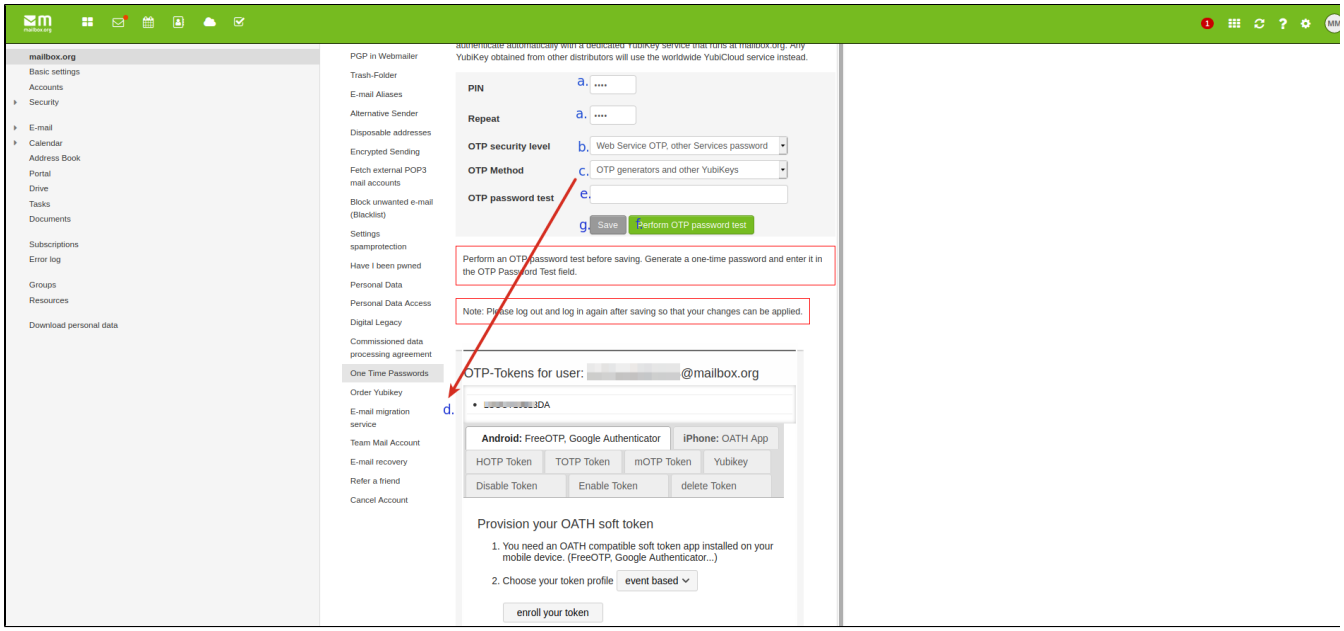
Make sure that both PIN fields contain the PIN before you continue.

b. Specify the desired **security level**.

We offer two different security levels for our two-factor authentication:

- **Web service OTP, other Services password:** This is the most common level for two-factor authentication at mailbox.org, and similar to how the majority of e-mail providers handle 2FA. You log in to the web interface using a PIN and one-time password. However, all other services such as IMAP, POP3, SMTP, WebDAV, CalDAV, CardDAV or ActiveSync will not use 2FA and require your (normal) password to be entered. You can continue to use local e-mail clients on your PC or smartphone, synchronize calendars with other devices, and so on.
- **Web service OTP, other Services off:** This is a security level for special use cases that is only available at mailbox.org. After choosing this option, you will only be able to log in to the web client at https://www.mailbox.org using a PIN and a one-time password. All other services will be disabled for your account. This also means that you cannot use local e-mail clients or synchronize any data with mailbox.org.

c. Select the OTP method: **OTP generators and other YubiKeys**



Screen snapshot: How to set up a soft token. For details on the individual steps a - g, please refer to the relevant descriptions in the text.

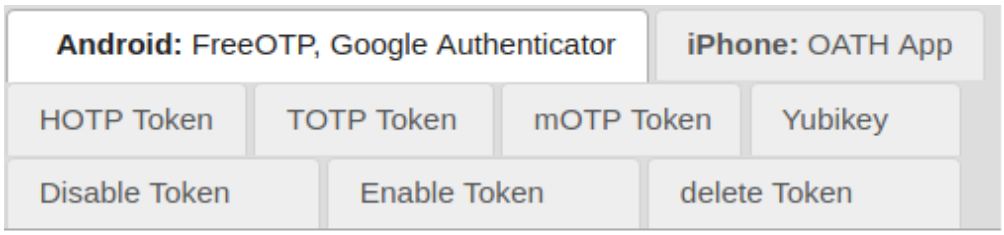
d. Create a token that will work with your device. It is usually safe to use any suggested setting.

Android: FreeOTP, Google Authenticator Also available to iPhone users through the iOS OTP app.

To continue, the required software needs to be installed on your device. Open the app and authorize camera access, if asked.

Click on the correct menu item to scan the QR code. With FreeOTP+, this can be achieved by accessing the three-dot menu in the upper-right corner of the screen.

Once QR scanning is working on your device, go back to the mailbox.org office and click on the button **enroll your token**. A QR code will appear on the page. Scan the QR code using the token generator app on your device.



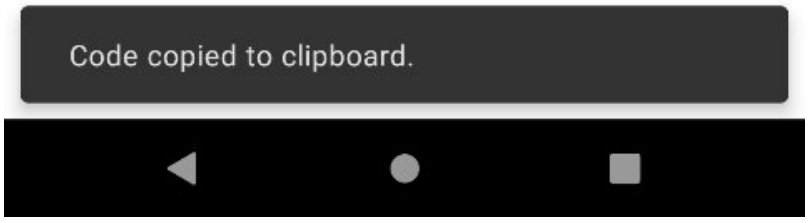
Provision your OATH soft token

1. You need an OATH compatible soft token app installed on your mobile device. (FreeOTP, Google Authenticator...)
2. Choose your token profile event based

   enroll your token
3. Install your soft token profile:

   To install the token on your mobile device, scan the QR code below with your soft token app or follow the link:

If everything went well, then the token will be displayed on your device's token generator app – the example below is from an Android 9 device, using FreeOTP+:



- Any tokens generated on our service are called LinOTP by default. You can rename the token by clicking on the three dots next to it. This can be useful when multiple tokens are used. Underneath the name of the token, you can see the token ID. This is also visible in the mailbox.org office and can be updated there, if necessary. As indicated in the screen snapshot above (the one with the QR code), soft tokens offer a choice between time-based (TOTP) and event-based (HOTP) methods.
- A time-based token expires after a certain period of time - usually represented by a timer, hour glass symbol, or similar - after which a new token is generated automatically.
  An event-based token is always created through user action (e.g., tapping a button). Such a token has a limited lifetime, too, but new tokens won't be generated automatically, but manually by the user.

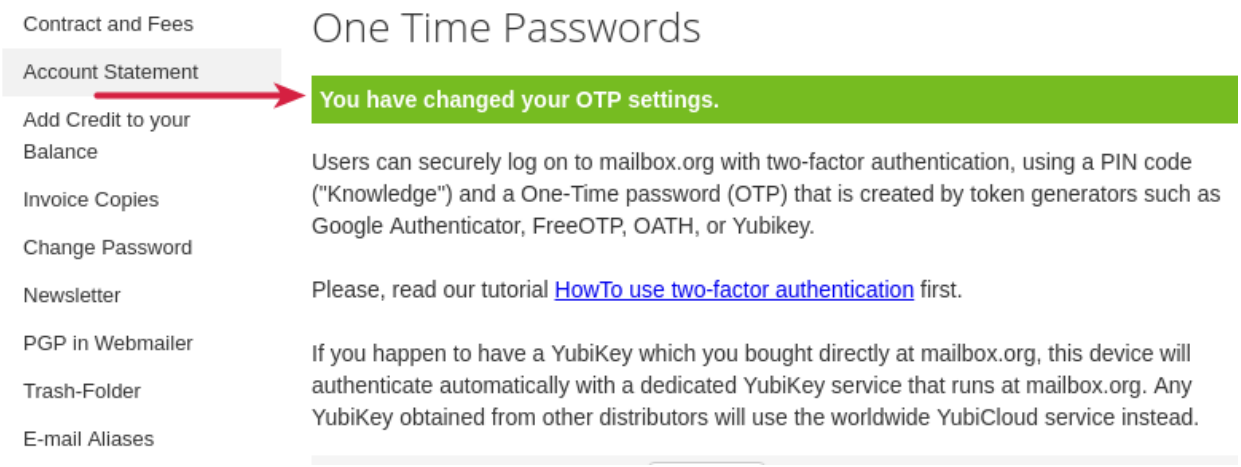
  Every now and then, it may happen that certain token apps do not work with one method or the other. In such case, we recommend you switch to another token type.

e. Click or tap on the token that you have just created in the token generator on your device. A new one-time password will be generated and there will also be timer counting down until the token expires.

f. In the mailbox.org web interface, enter the one-time password into the OTP password test field and click on the button **Perform OTP password test** – note that you must do this before the countdown in your app finishes. Don't worry if you missed the time window on your first attempt – you can always create a new token and try again see step e.

g. If the test completes successfully, click on the **Save** button (Its color will have changed from grey to green).

Please note the success message at the top of the page:



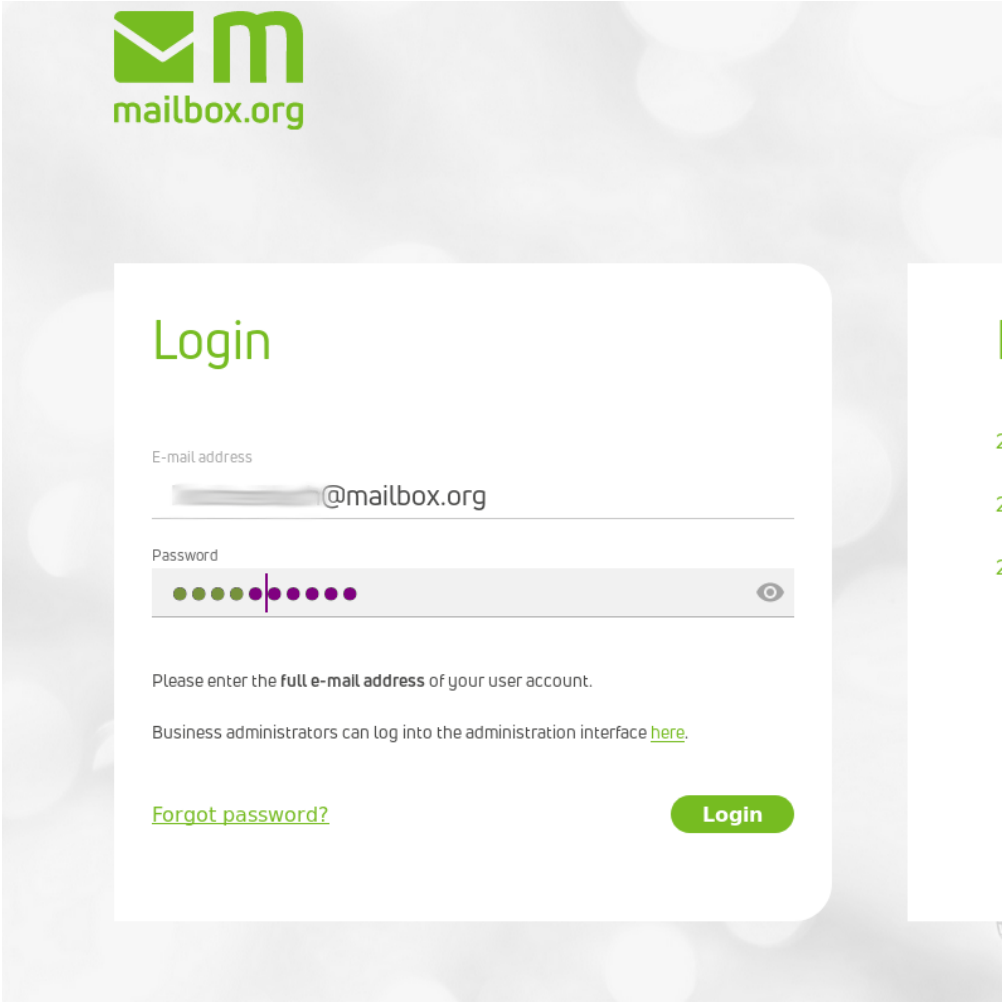
Finally, log out to finish the setup.

Your two-factor authentication is now active. From now on, you will log in with your PIN in combination with the one-time password.

If the test has not been successful, please repeat the token setup.

Please note that both the PIN and the OTP must be entered into the same password field.

Please see the screen snapshot below: Enter the **4-digit PIN** first and then continue straightaway with the **one-time password** from your YubiKey or token generator. Do NOT insert a space between the two entries.



If you lose your token, it may still be possible to reset your password, provided you set up a password recovery method BEFOREHAND. If you did, then it will be possible for you to reset your password by e-mail or text message, for example, after which you can create a new password. Doing this will also disable two-factor authentication for your account: You will now log in using only your newly created account password and can access all features of your mailbox.org office as usual.

It is only possible to have your password reset if the necessary password recovery information has been specified beforehand. If you did not provide an e-mail address or a mobile phone number as a means to reset your password, perhaps to remain fully anonymous, and if access to your mailbox.org e-mail account via IMAP has been deactivated, then there is no way for us to verify your identity and confirm you are the owner of the account.
Note that in such a case, a password reset will not be possible!

In order to be able to activate, deactivate or delete a token, you have to select a token in the first place. This is not possible with the keyboard.

Currently we offer this workaround: Deactivate CSS in your browser. In Firefox this is done by hitting "alt", so that the menu bar appears on top **view page style no style**.
Now search the respective token and confirm with "enter". Now you may reactivate CSS and the token will appear correctly.

Related Articles

- How to use two-factor authentication - 2FA