How to use two-factor authentication - 2FA

2FA also works if you use your own domain with mailbox.org

For your security, mailbox.org supports several variants of two-factor authentication:

1. The best and most secure solution is to buy a mailbox.org YubiKey directly from us. This special YubiKey will authenticate your identity by connecting to a dedicated YubiKey server in our data center. No data is transferred to third parties.
   
   In general, hardware tokens offer better security than software solutions on a mobile phone. See the FAQ article about YubiKeys for further details.

2. Alternatively, you can use a generic Yubikey bought from Yubico. This key will perform authentication using the world-wide YubiCloud service.

3. With a hardware token: you can use HOTP or TOTP compatible tokens like "Nitrokey Pro or Nitrokey Storage" for the login to our web interface.

4. As a third variant, users may opt for any OATH-, TOTP-, HOTP- oder mOTP-compatible token generator such as those employed by smartphone apps like FreeOTP, Google Authenticator, or OATH Token.

We do not offer SMS based 2FA and this is not planned for the future.

The 2 factor authentication is only available for our web interface. The other services like IMAP, POP3, SMTP and also WebDAV, CalDAV and CardDAV do not support 2FA.

Please ensure to allow the needed cookies in your web browser.

Important: If you loose your Yubikey or your token, you can only reset your password (and switch off 2FA), if you provided some information for the password reset procedure. Otherwise, we cannot help.

mailbox.org login with PIN and One-Time-Password

If you want to log in with PIN and OTP password in our mailbox.org office web interface, you have to enter the 4-digit PIN and the One-Time-Password for password input without any whitespace char. (PIN+Token entered into the “Password” field)

If you use two-factor authentication, the following restrictions apply:

- You cannot change your main e-mail address as long as you have selected one of the two OTP options under "Settings -> mailbox.org -> One Time Passwords -> OTP backup level".
  If you want to change the main e-mail address, you must first change the option "OTP security level" to "Off, use normal passwords only". Then you can change the main e-mail address and log back in with it. Finally, reset your OTP security level as desired. We are working on a bugfix.

- You cannot log in to the mailbox.org office with several browsers or devices at the same time using a web client.

- By using two-factor authentication, you can only log on once at a time.

- You must log out before closing the browser.
  Although it should be common practice to log off before closing the browser, it is absolutely necessary when using one-time passwords!
Otherwise you will receive an error message the next time you log in.

If you get this error message, please log off. Then you should be able to log in correctly. Please remember to log off correctly in the future.

If you set the OTP backup level to “OTP only for web interface, all other services off”, logging into our helpdesk and the user forum is no longer possible!

Configuration of PIN and OTP password

In mailbox.org Office you can select the desired authentication method under “Settings -> mailbox.org -> One Time Passwords -> OTP Method”:

- Specify the **four-digit PIN** and the desired **security level**. The PIN may contain letters (a-z lowercase or uppercase) and numbers, but no special characters. Then select the desired method to generate one-time passwords: via mailbox.org-YubiKey or with one of the other methods.

We offer two different levels of two-factor authentication:

1. **Webinterface OTP, everything else password**: With this option you set up mailbox.org so that it works like most other e-mail providers with two-factor authentication. You can log in to the web interface with your PIN and one-time password and continue to use all other services such as IMAP, POP3, SMTP, WebDAV, CalDAV, CardDAV or ActiveSync with your (normal) password. So you can continue to use local email clients on your PC or smartphone, synchronize calendars, etc.
2. **OTP only for web interface, all other services off**: This is a special feature of mailbox.org. If you select this option, you can only log in to the web client, the mailbox.org office with secret code and one-time password. All other services will be deactivated for your account. You will not be able to use local email clients or synchronize data.

**First click on “Submit Query”. Be sure to create or activate an OTP token.**

**Manage your own OTP token**
When selecting the option **OTP-generators and other YubiKeys**, an additional tool for managing your OTP tokens will be displayed.

Here, you can see tabs that offer options for the quick configuration of Android or Apple smartphones; followed by expert settings for the configuration of arbitrary compatible tokens and for registering third-party YubiKeys; and actions for the management of existing tokens (Enable/Disable/Delete).

<table>
<thead>
<tr>
<th>Android: FreeOTP, Google Authenticator</th>
<th>iPhone: OATH App</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOTP Token</td>
<td>TOTP Token</td>
</tr>
<tr>
<td>mOTP Token</td>
<td>Yubikey</td>
</tr>
<tr>
<td>Disable Token</td>
<td>Enable Token</td>
</tr>
<tr>
<td></td>
<td>delete Token</td>
</tr>
</tbody>
</table>

**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:

   ![QR Code](image)

   After having created an OTP token for a smartphone app, just scan the QR code with your phone to set up the app for generating valid tokens.

Lost token - what now?
If you have lost your token, you can still use the function to reset your password. The moment you reset your password e.g. by e-mail or a reset code via SMS, you can create a new password. This also deactivates two-factor authentication. With this new, regular password you can log in again - and have access to all functions of your mailbox.org office as usual.

As already mentioned above, you can only reset your password if you have stored the corresponding information in your account. If, for example, you have not entered an e-mail address or a mobile phone number for a password reset for reasons of anonymity and access to your mailbox.org e-mail account via IMAP is deactivated, then we have no way of verifying your identity as the owner of the account.

In this case a password reset is no longer possible!

Don't forget to click "Submit" yet.

Related Articles

- How to use two-factor authentication - 2FA

If you use two-factor authentication, the following restrictions apply