

2FA - Two-factor authentication for your mailbox

Two-factor authentication, or **2FA** as it's commonly abbreviated, adds an extra step to your basic login procedure. Without 2FA, the password is your single factor of authentication: you enter your username and password, then you're done.


With 2FA, you log in to the Webmail by entering your username and password and the six-digit code provided by an app installed on your smartphone.

On this page

1. [Enable 2FA for your mailbox](#)
2. [Disable 2FA for your mailbox](#)

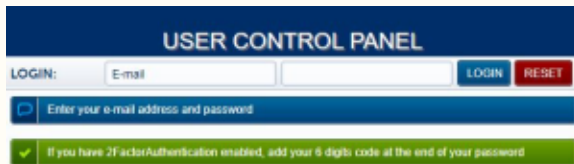


After the latest update of the GroupOffice Webmail, you will be prompted to enter the 2FA code in a new pop-up window.



When logging into the [User Panel](#), if you have 2FA enabled for your mailbox, you must add at the end of the password the 6-digit code provided by the app on your phone.

For example, if your password is **T9D3K!px** and the 6-digit code is **189 145**, you must enter **T9 D3K!px189145** in the login form of the User Panel.



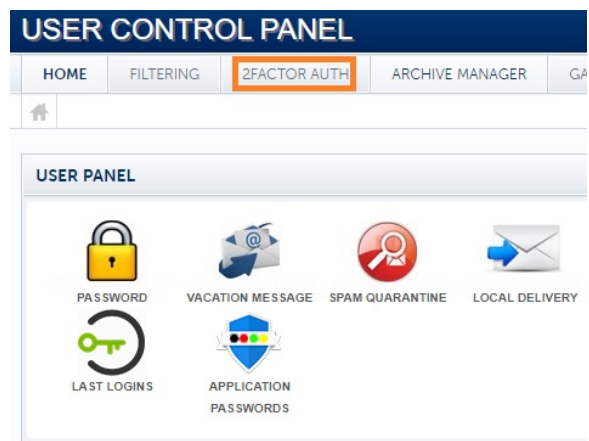
1. Enable 2FA for your mailbox

What you need:

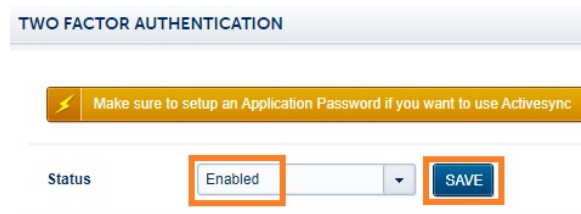
- a smartphone with a 2FA App installed (OTP / 2-Step Verification / 2-Factor Authentication), such as [Authy](#) or [Google Authenticator](#).

To enable 2FA for your e-mail address:

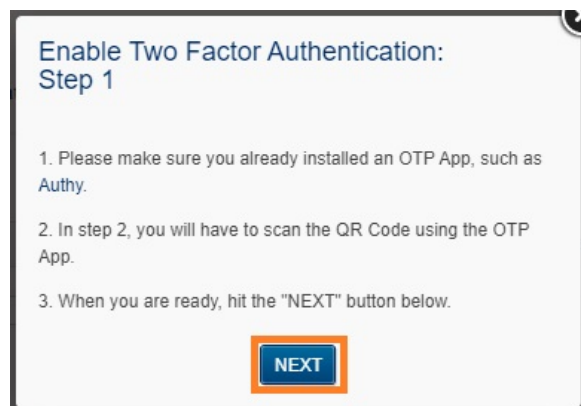
- Log in to the [User Panel](#)
- From the menu, go to **2-Factor Auth**



- Update the dropdown **Status** to **Enabled**. Click on the **Save** button.



- Recheck the requirements: have a 2FA App installed on your phone, such as [Authy](#) or [Google Authenticator](#)
- When ready, click on the **Next** button



- Scan the QR code with the installed 2FA App and fill in the generated six-digit code in the **Challenge** input field.
- **Click on the Save button before your token expires. It is always better to wait for the app to generate a fresh token, so you have enough time before it expires.**
- You have enabled 2FA, and you will be prompted to fill in the token every time you log in using Webmail.

Enable Two Factor Authentication: Step 2

1. Scan this QR code using your OTP App.
2. Once the account is added, you will be given a 6 digit code
3. Enter the code in the field below.
4. Hit "SAVE" button below before your code expires.



Challenge

2. Disable 2FA for your mailbox

To disable 2FA for your e-mail address:

- Log in to the [User Panel](#)
- From the menu, go to **2-Factor Auth**

USER CONTROL PANEL

HOME FILTERING **2FACTOR AUTH** ARCHIVE MANAGER G&A

USER PANEL

PASSWORD VACATION MESSAGE SPAM QUARANTINE LOCAL DELIVERY

LAST LOGINS APPLICATION PASSWORDS

- Update the dropdown **Status** to **Disabled**. Click on the **Save** button.

TWO FACTOR AUTHENTICATION

Make sure to setup an Application Password if you want to use Activesync.

Status

- Insert the token from your 2FA App (such as Authy or Google Authenticator) in the **Challenge** input field.
- **Click on the Save button before the token expires. It is always better to wait for the app to generate a fresh token, so you have enough time before it expires.**
- After you see the confirmation message that the 2FA was disabled, you can delete the entry from your 2FA app.

Disable Two Factor Authentication

1. To disable 2 Factor Authentication, insert the code from your OTP App (Authy).

2. Hit "SAVE" button below before your code expires. If this happens, insert again your newly generated code from Google Authenticator app.

Challenge

SAVE