

# 2FA - Two-factor authentication

**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 Admin Panel by entering your username and password and the six-digit code provided by an app installed on your smartphone.



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

## On this page

[Enable 2FA for the Admin Panel](#)  
[Disable 2FA for the Admin Panel](#)

## Enable 2FA for the Admin Panel



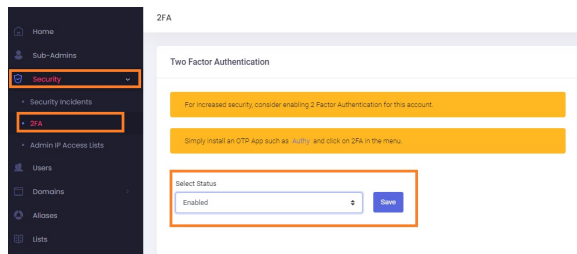
If you're using this Admin account as credentials for the API, the API login will fail after enabling 2FA. To solve this, create a Sub-Admin with special permissions for the API authentication only.

### What you need:

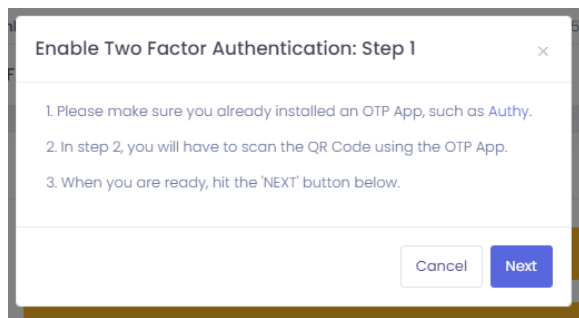
- a smartphone with a 2FA App installed (OTP / 2-Step Verification / 2-Factor Authentication), such as [Authy](#) or [Google Authenticator](#).

To enable 2FA for your Admin account:

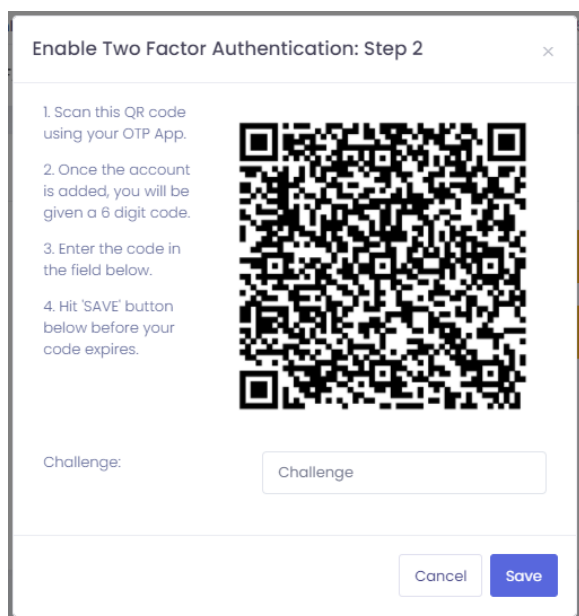
- Log in to the [Admin Panel](#)
- From the menu, go to **Security 2FA**
- Update the dropdown **Select Status** to **Enabled**. Click on the **Save** button.



- Recheck the requirements: have a 2FA App installed on your phone.
- When ready, click on the **Next** button.



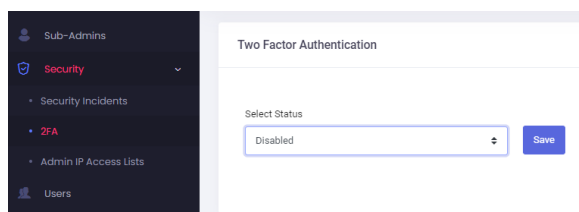
- Scan the QR code with the installed 2FA App and fill in the generated six-digit code in the **Challenge** input field.
- **Click on the Save button before your token expires.**



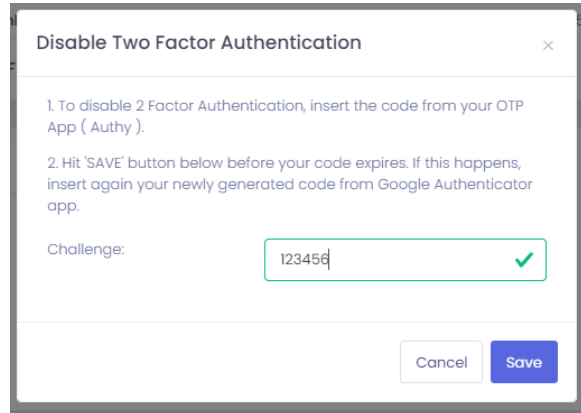
## Disable 2FA for the Admin Panel

To disable the 2FA for your Admin account:

- Log in to the [Admin Panel](#)
- From the menu, go to **Security 2FA**
- Update the dropdown **Select Status** to **Disabled**. Click on the **Save** button.



- 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.**



The screenshot shows a modal dialog box titled "Disable Two Factor Authentication" with a close button (X) in the top right corner. The dialog contains two numbered instructions: "1. To disable 2 Factor Authentication, insert the code from your OTP App ( Authy )." and "2. Hit 'SAVE' button below before your code expires. If this happens, insert again your newly generated code from Google Authenticator app." Below the instructions, there is a label "Challenge:" followed by a text input field containing the code "123456". A green checkmark is visible to the right of the input field, indicating the code is valid. At the bottom right of the dialog, there are two buttons: "Cancel" and "Save".

- After you see the confirmation message that the 2FA was disabled, you can delete the entry from your 2FA app.