Fube

GUIDE

How to enable two-step verification (2FA) in Fube



How to enable two-step verification (2FA) in Fube

> Your Fube account holds the most sensitive parts of your business: invoices, customers, amounts and the paperwork you prepare for the tax authorities. A password on its own — one that gets reused, jotted down in a note or sent over chat — is a weak lock for all of that. Two-step verification (2FA) adds a second check when you sign in: as well as your password, it asks for a temporary code on your mobile that changes every few seconds. This guide takes you through it from start to finish: enabling it, confirming the code, saving your recovery codes and, later on, regenerating them or disabling it.

Before you start you need three things. First, a **standard authenticator app (TOTP)** installed on your mobile: Google Authenticator, Authy, 1Password or an equivalent. To sign in, Fube doesn't use SMS or email codes: the second factor is always the one from an app of this kind. Second, **access to your account's email**: to confirm that it's really you enabling it, Fube sends you a code there. And third, a safe place to store the **recovery codes** Fube will give you at the end — for example, your company's password manager. 2FA is **optional**, but it's especially advisable for accounts with the **Owner** or **Administrator** role, which have the most access to invoicing. You can see the full scope of these controls on the account security page.

Step 1. Open your profile's security settings

Sign in to Fube with your account and go to **My profile › Security**. There you'll find the **Two-step verification** card, with a label showing its status: *Disabled* if you haven't set it up yet. Below it, Fube explains that 2FA adds an extra layer and that, once enabled, it will ask for a temporary code as well as your password every time you sign in. Click the **Enable two-step verification** button.

Step 2. Scan the QR code with your authenticator app

Fube generates and displays a **QR code**. Open your authenticator app, choose to add a new account and scan the QR code with the camera. The app will register Fube and start generating six-digit codes that refresh automatically every few seconds.

If you can't scan the QR code (for example, because the app is on the same device), Fube shows a **key to enter manually** below it. Copy it with the copy button and paste it into your app as the ‘setup key’. Once the app is showing the Fube code, click **Continue**.

Step 3. Confirm with the six-digit code

Fube moves on to the verification screen, which asks for **two six-digit codes**:

- **The one from your authenticator app**, in the first boxes: the one you can see at that moment. As it expires after a few seconds, enter the one that's visible at that exact instant; if you've taken too long, wait for the next one and use that.
- **The one from your email**, below. Click **Send code** and Fube sends one to your account's address; type it into the second row of boxes. If it doesn't arrive, after 30 seconds you can click **Resend code**.

Click **Enable**. The email code isn't a mere formality: once 2FA is enabled, your app's code is used to confirm sensitive changes to your account, so Fube checks that the person setting up the app is the person who reads your inbox, and not someone who has found your session left open.

If the code is correct, Fube confirms that two-step verification has been enabled. If you get an incorrect code error, check which box it flags: if it's the app one, make sure that the time on your mobile is set to sync automatically (TOTP codes depend on the time) and enter the current code again; if it's the email one, check that you've typed the most recent one you received.

Step 4. Save your recovery codes

As soon as it's enabled, Fube opens the **Backup codes** window with the list of codes. They're your plan B: they let you in even if you lose your mobile or can't generate a code with the app. Treat them with the same care as a password.

You have three options in that window:

- **Copy** the codes to the clipboard to paste them into your password manager.
- **Download** a text file (`fube-backup-codes.txt`) containing all the codes.
- Click **I've saved my codes** once you've stored them safely.

Each recovery code **can only be used once**. Keep them in a safe place, separate from the mobile that has your authenticator app. If you lose them, you can generate new ones later (see 'Ongoing management').

With that, 2FA is active: from your next sign-in, Fube will ask you for the code from your app as well as your password.

Step 5. Repeat it for the accounts with more permissions

Two-step verification protects one account at a time: each person's own. That's why it's advisable for anyone with the **Owner** or **Administrator** role to enable it on their own profile by following these same steps: these are the accounts with the most access to invoicing and the ones most worth locking down. How that access is shared out across the team is managed in the **members and roles** section, within the **team and permissions** controls: that way each person signs in with their own account and their own second factor, without sharing passwords.

Ongoing management: regenerating codes or disabling 2FA

Once it's enabled, the card in **My profile › Security** changes and shows how many **backup codes you have left** (the *Backup codes* label with the *remaining codes*). From there you can do two things, and both are confirmed in the same way: with a **verification code** that you choose how to obtain. With 2FA enabled, Fube lets you choose between **Email code** (you click **Send code** and it arrives at your account's address) and **Authenticator app** (you type the one your app is showing at that moment). Your password isn't requested: anyone who had it couldn't make these changes without your inbox or your mobile.

- **Regenerate backup codes.** If you've used several, lost them or simply want new ones, click **Regenerate codes** and confirm with the code. Fube generates a new set and **the previous ones stop working**, so save them again.
- **Disable two-step verification.** Click **Disable** and confirm with the code. Bear in mind that your account will be less protected without 2FA, so only do this if you have a clear reason.

The email code **expires after 15 minutes** and is only valid for the action you requested it for: one requested to regenerate the codes can't be used to disable 2FA.

The other half of the lock: your password

2FA is the second factor, but the first is still your password, and that's also managed from **My profile**.

To change it, go to **My profile › Password**. It asks for the **new password** twice and a **verification code**: click **Send code** and type the one that arrives by email, or, if you have 2FA enabled, choose **Authenticator app** and use the one from your app. It doesn't ask for your current password, and that's deliberate: anyone who has worked it out, or anyone who sits down at your computer with the session open, can't change your access without your inbox or your mobile.

If you can't remember it, there's no need to contact us. On the sign-in screen there's **Forgot your password?**, and from there it's three steps: you enter your email, Fube sends you a **six-digit code**, you type it in and choose your new password. It's a code, not a link, so have it to hand when you open the email.

One detail worth knowing if you manage a team: **the welcome email never contains a password**. If you create someone's account directly, it's up to you to give them the initial password through a secure channel.

Edge cases and common errors

- **The code always comes up as 'incorrect'.** It is almost always a time issue: TOTP apps and Fube must share the exact same time. Turn on automatic date and time on your phone and try again with the current code.
- **You have changed phones.** If 2FA is still active, sign in with a **recovery code**, disable it by confirming with the **email code** (you no longer have the app on your old phone) and enable it again to register the app on the new device. That is why it is essential to have saved the codes beforehand.
- **The email code does not arrive.** Check your spam folder and make sure it is the address on your account: Fube tells you which one it was sent to. After 30 seconds you can request another with **Resend code**; if you request many in a row, Fube will make you wait a few minutes. Always use the most recent one you have received.
- **You have lost your phone and your recovery codes.** Without either of them you will not be able to generate the second factor yourself; you will need to contact Fube support to regain access. Saving your recovery codes from the outset avoids precisely this situation.
- **You do not want to use the same app for everything.** Any standard TOTP app will do; you can choose the one you already use for other services. Fube does not require any particular one.

Frequently asked questions

Is it mandatory to enable two-step verification?

No. In Fube, 2FA is **optional**. It is highly recommended, especially for accounts with the Owner or Administrator role, but you can keep using Fube with just a password if you prefer.

Which app do I need?

Any standard **TOTP** authentication app: Google Authenticator, Authy, 1Password or other equivalents. To sign in, Fube does **not** send codes by SMS or email: the second factor is always generated in an app of this kind. The codes that do arrive by email are something else: they confirm sensitive changes to your account, such as enabling or disabling 2FA or changing your password.

What happens if I lose the phone with the app?

That is what the **recovery codes** Fube generates when you enable 2FA are for: they let you sign in even if you do not have the device. Each one can be used only once, so it is best to store them somewhere safe from the start and regenerate them if they run out.

Does this have anything to do with Verifactu?

They are different things. 2FA protects **who accesses** your account; Verifactu regulates **how invoices are issued and recorded**. The obligation to use an invoicing system compliant with Verifactu arrives on **1 January 2027** for companies and on **1 July 2027** for all other businesspeople, professionals and self-employed workers. If you want to get up to speed on that side of things, the guide to **getting started with Verifactu** explains it without jargon.

Give your account its second key

Enabling two-step verification takes a couple of minutes and leaves your invoicing much better protected. If you do not use Fube yet, you can **create your free account** and set up 2FA from day one.

Fube

START TODAY

Put this into practice with Fube

Create your free account and issue your first Verifactu-compliant invoice in minutes. No card, nothing to install.

fube.es

Invoicing and business management for freelancers and SMEs in Spain