Setting Up Two-Factor Authentication (2FA)

Admin · https://coreel.ai/help/setting-up-two-factor-authentication-2fa/

Two-factor authentication adds a second layer of protection to your coReel account. After you enter your password, you'll also need a 6-digit code from an authenticator app on your phone. Even if someone learns your password, they can't sign in without your phone.

This article walks you through enabling 2FA, signing in with it, and what to do if you lose access to your authenticator.

What you'll need

- A smartphone with an authenticator app installed. We recommend **Google Authenticator**, **Microsoft Authenticator**, or **1Password**. Any TOTP-compatible app will work.
- 2-3 minutes to complete setup.
- A safe place to store your recovery codes (we'll explain).

Step 1 — Open your security settings

1. Sign in to coReel at app.coreel.ai.
2. Click your profile icon in the top right and choose **Settings**.
3. Find the **Two-Factor Authentication** card.
4. Click **Enable 2FA**.

Success Check: You should see a QR code on the screen along with a long string of letters and numbers below it.

Step 2 — Scan the QR code in your authenticator app

1. Open your authenticator app on your phone.
2. Tap the option to **add a new account** (the icon varies by app — usually a `+` or scanner icon).
3. Choose **Scan QR code**.
4. Point your phone at the QR code on your screen.

If you can't scan the code, tap **Enter setup key manually** in your app and type the long string shown below the QR code. The account name will be `coReel`.

Success Check: Your authenticator app should now show a 6-digit code that changes every 30 seconds.

Step 3 — Verify and save your recovery codes

1. Type the current 6-digit code from your authenticator into the **Verification code** field in coReel.
2. Click **Verify and enable**.
3. You'll be shown a list of **recovery codes**. These are one-time-use codes you can use if you lose access to your phone.

Important: Save your recovery codes somewhere safe right now — a password manager, a printed copy in a locked drawer, or a secure note. Do not save them in plain text on the same device you use to sign in.

Each recovery code can only be used once. After it's used, it's gone.

Success Check: Your Settings page should now show "Two-Factor Authentication: Enabled."

Signing in with 2FA enabled

The next time you sign in:

1. Enter your email and password as usual.
2. On the next screen, open your authenticator app and type the current 6-digit code.
3. Click **Verify**.

You're in.

If your code doesn't work, double-check that your phone's clock is set to automatic time. TOTP codes are time-based, so a clock that's drifted by more than 30 seconds will produce invalid codes.

I lost my phone — how do I get in?

Use one of the recovery codes you saved during setup.

1. On the verification screen, click **Use a recovery code instead**.
2. Type one of your saved codes.
3. Sign in.

Once you're in, immediately go to **Settings → Two-Factor Authentication** and re-enroll with your new device. This invalidates the old setup and generates fresh recovery codes.

If you've also lost your recovery codes, contact support — we'll verify your identity through other means before resetting 2FA on your account.

Disabling 2FA

If you need to turn 2FA off (we don't recommend it):

1. Go to **Settings → Two-Factor Authentication**.
2. Click **Disable 2FA**.
3. Enter your password and a current 6-digit code from your authenticator to confirm.

Troubleshooting

My code keeps being rejected. Check your phone's clock settings. Both your phone and our server use UTC time; if your phone's clock has drifted, codes will fail. Switching your phone to automatic/network time usually fixes it.

My QR code expired before I could scan it. Just click **Generate a new code** on the setup screen and start again.

I'm an admin and was forced to enable 2FA before I could continue. Admin accounts on coReel require 2FA for security. This is required for all team owners and managers — there's no opt-out.

Pro tips

- Use a password manager that doubles as a TOTP authenticator (like 1Password or Bitwarden) so your codes and passwords are backed up together.
- Print one set of recovery codes and keep them in a fireproof safe or with your other critical documents.
- If you set up 2FA on a shared work computer, sign out of the authenticator app browser session when you're done.