

Two-factor authentication setup in Better Studio

Starting with Better Studio version 3.15, **two-factor authentication (2FA) is required for all accounts**. This guide explains what 2FA is, how it works in Better Studio, and how to set it up using your preferred verification method.

Two-factor authentication adds a second layer of security to your account. In addition to your password, you will be asked to provide a six-digit one-time code each time you sign in. This code is generated by an authenticator app on your mobile device.

Supported verification methods

- **FreeOTP** (recommended for open-source environments)
- **Google Authenticator**
- **Microsoft Authenticator**

Note

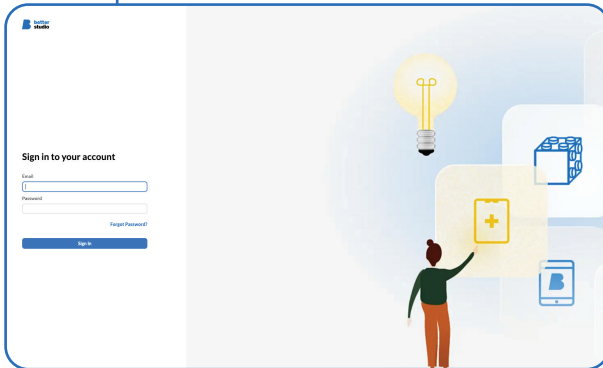
Codes are six digits long and valid for 30 seconds.
Keep your device on hand when signing in.

Account logout

For security reasons, your account will be permanently locked after five consecutive failed sign-in attempts. A lockout can be reset after 12 hours. If you are locked out, follow the steps in the **Troubleshooting section** at the end of this guide.

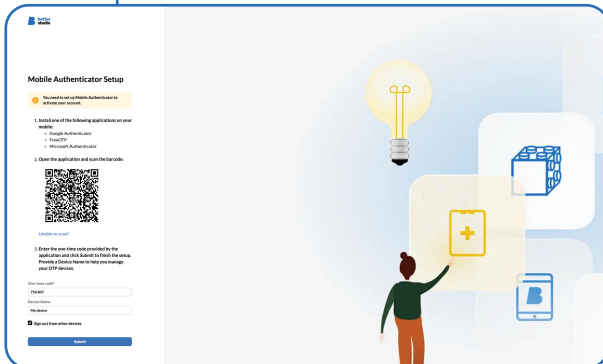
Setting up 2FA in Better Studio

When you sign in to Better Studio for the first time after the 3.15 release, you will be prompted to configure two-factor authentication. Follow the steps below.



Step 1: Sign in to Better Studio

Open Better Studio in your browser and enter your username and password as usual.



Step 2: Set up your verification method

After entering your credentials, you will see the two-factor authentication setup screen.

A QR code will be visible on the screen.

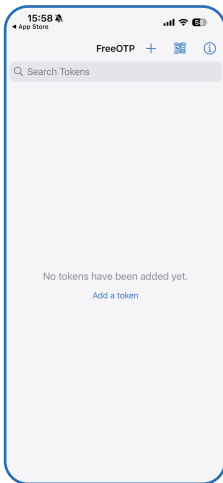
Follow the instructions in this guide to set up the authentication app you are using.

FreeOTP

FreeOTP is a free, open-source authenticator app developed by Red Hat. It is available for Android and iOS.

Download FreeOTP:

- **Android:** [Google Play Store](#)
- **iOS:** [Apple App Store](#)



Step 1: Open FreeOTP on your mobile device.

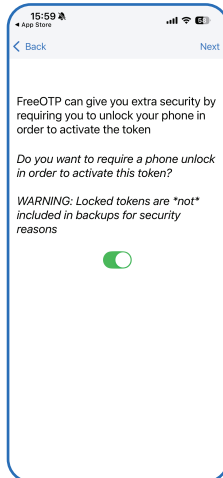
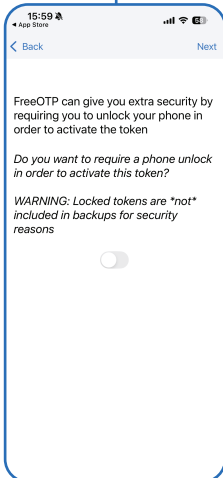
If this is the first time you are using FreeOTP, the token list will be empty.

Step 2: Tap the scan icon.

Tap the QR code icon (or the camera icon, depending on your device) at the top of the screen to open the QR scanner. You can also click on “Add a token”.

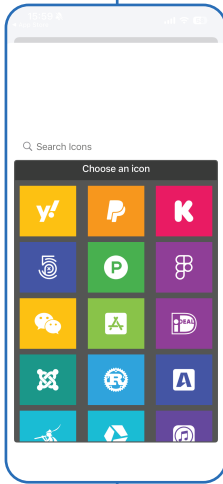
Step 3: Scan the QR code displayed in Better Studio.

Point your device's camera at the QR code shown on the Better Studio 2FA setup screen. FreeOTP will detect and import the account automatically.



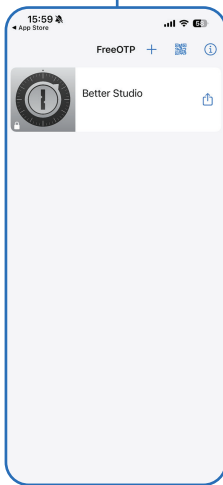
Step 4: Confirm additional security.

After scanning, you will be prompted to choose whether you want additional security for the token access. If you want FreeOTP to enable phone unlock in order to activate this token, toggle the option. You can skip this step by clicking “Next”.



Step 5: **Choose an icon**

Next, you will be able to choose an icon for your new Better Studio access token. There is no special Better Studio icon, but you can choose one from the list of provided ones.



Setup complete!

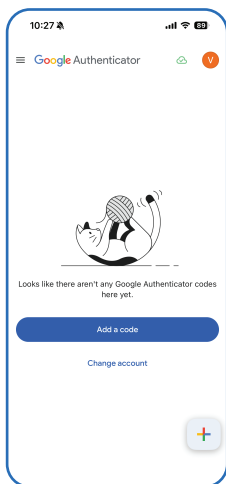
FreeOTP will generate a new code each time you sign in.

Google Authenticator

Google Authenticator is a free authenticator app available for Android and iOS.

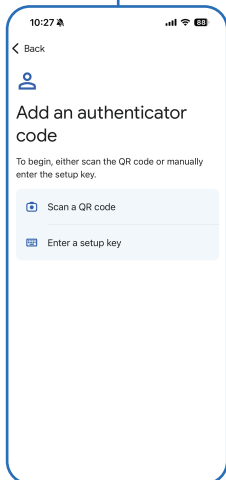
Download Google Authenticator:

- **Android:** [Google Play Store](#)
- **iOS:** [Apple App Store](#)



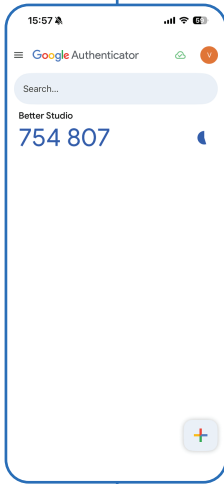
Step 1: **Open Google Authenticator and tap the add button.**

Open the app on your mobile device. Tap the + icon (bottom right on Android, or the menu on iOS) or click on “Add a code” to add a new authentication code.



Step 2: **Select "Scan a QR code".**

From the options presented, select **Scan a QR code**. Grant camera access if prompted.



Step 3: **Scan the QR code and enter the verification code.**

Point your camera at the QR code shown on the Better Studio 2-factor authentication setup screen. Google Authenticator will import the account and immediately begin displaying a six-digit code.

Setup is complete. Google Authenticator will generate a new code each time you sign in.

Tip

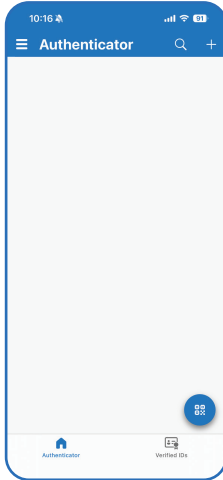
You can optionally sign in to your Google Account within Google Authenticator to sync your codes across devices.

Microsoft Authenticator

Microsoft Authenticator is a free app available for Android and iOS.

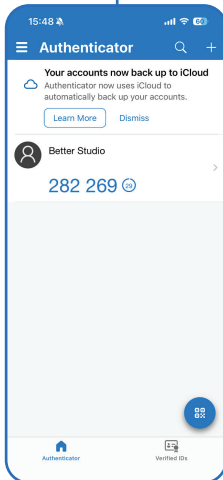
Download Microsoft Authenticator:

- **Android:** [Google Play Store](#)
- **iOS:** [Apple App Store](#)



Step 1: Open Microsoft Authenticator and tap "Add account".

Open the app on your mobile device. Tap the **+** icon in the top right corner, then select **Other account (Google, Facebook, etc.)**.



Step 2: Scan the QR code and enter the verification code.

Select **Scan QR code** when prompted. Point your camera at the QR code shown on the Better Studio 2-factor authentication setup screen.

Microsoft Authenticator will import the account and display a six-digit code.

Setup is complete. Microsoft Authenticator will generate a new code each time you sign in.

Signing in after 2FA is enabled

Once 2FA is configured, every sign-in to Better Studio follows this process:

1. Enter your username and password.
2. Open your authenticator app.
3. Enter the six-digit code in the "One time code" field.
4. Select **Sign in**.

The code is valid for 30 seconds. If the code expires before you submit it, wait for a new code to appear and use that instead.

Troubleshooting

My code is not being accepted

Check that the time on your mobile device is correct and set to your local time zone. TOTP codes are time dependent. A clock that is out of sync will generate invalid codes.

If your code is active, but it's still not accepted, you can try to delete your cache and browser history.

I have been locked out of my account

Accounts are locked after five consecutive failed sign-in attempts. Lockouts reset automatically after 12 hours. If you need access sooner, contact support:

Free users: Post in the [Better Studio community on Better Hive](#).

Paid users: Raise a ticket via [Zendesk support](#).

I have changed my mobile device and can no longer access my authenticator app

Contact support to reset your 2FA configuration. Your account administrator can reset your 2FA settings so that you can reconfigure it on your new device.

