Two Factor Authentication for Front End Use

Setting up 2FA for Your App

You can now choose between further security options for your events. These extra options are only available for private and secure platforms that require login.

Security options are as follows:

Disabled

This is the login process as you currently know it, with no changes. Users will not be given the option to set up 2FA during the login process.

Optional

After going through the standard process of inputting their email and password, users will be given the option to set up a 2FA device at login, but it is not compulsory. They can opt for 'ask me later' if they don't want to do it at that moment, or they can select 'don't ask me again' in which cse this screen will never appear again when logging into the app.

For setting up a device, please see the option for usng an authentication app below.

Email verification

This option means that 2FA is required, however front-end users can choose between an authentication app, or verification via a code being sent to their email.
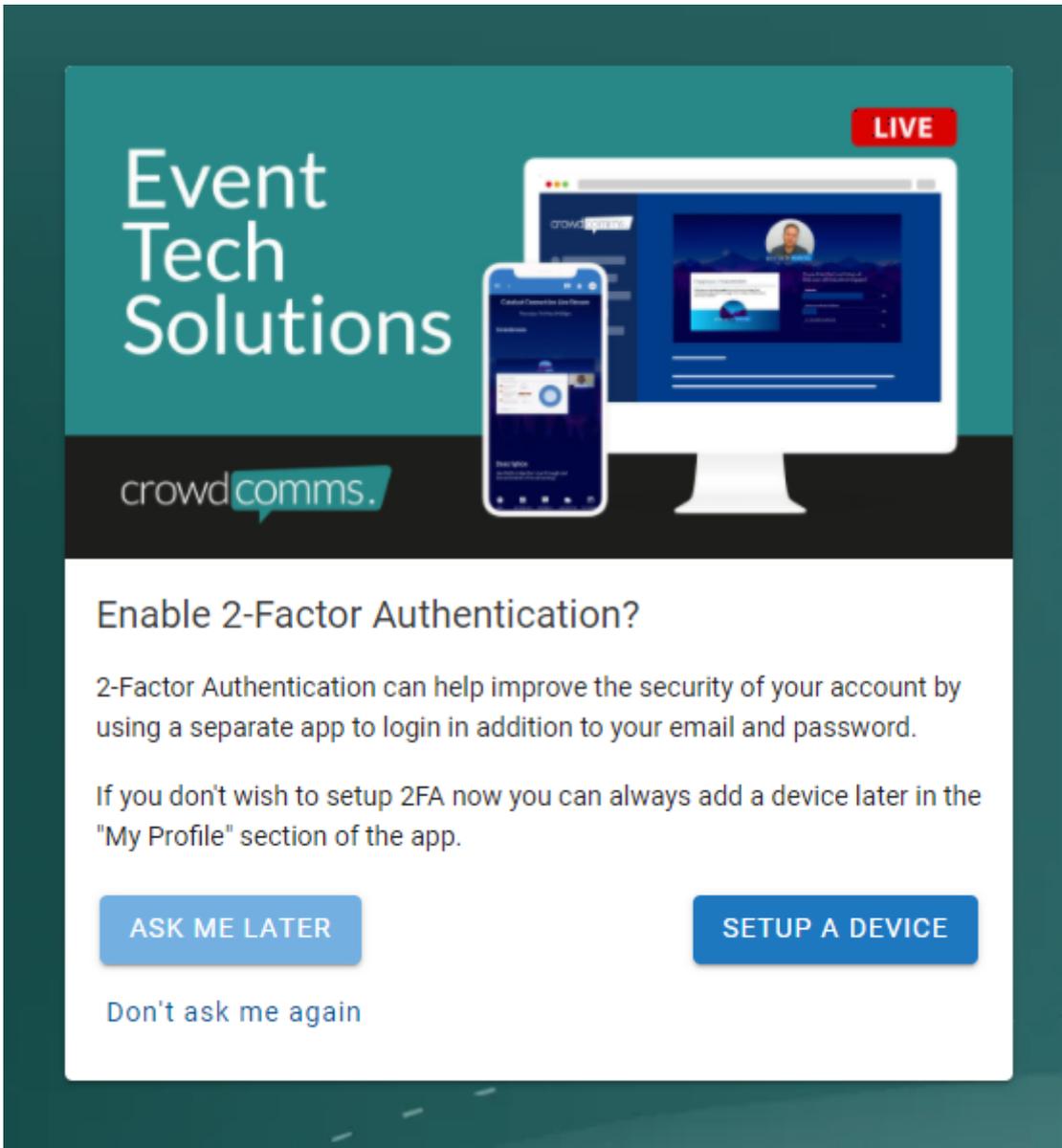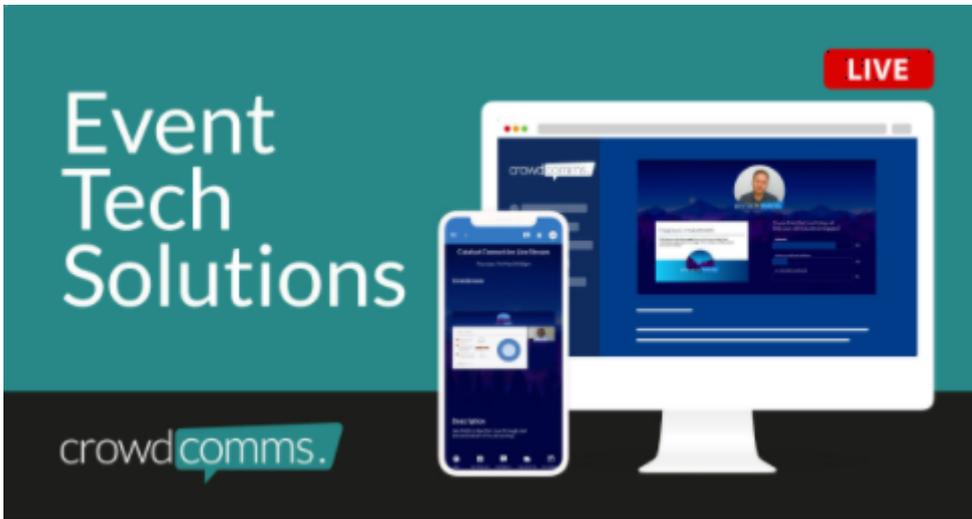
This app requires 2-Factor Authentication

2-Factor Authentication can help improve the security of your account by using a separate app to login in addition to your email and password.

If you don't wish to setup 2FA now, we'll send a verification code to your registered email address instead.

SETUP A DEVICE　　　　　　　　**EMAIL ME A CODE**

If they choose to receive a code, then a 6-digit code will be sent to their email which they will need to input before proceeding:

Please check your email

We've sent a unique 6-digit code to your registered email address. Please enter the code into the box below to proceed.


☐ Trust this device for 30 days

CANCEL   **NEXT**

Didn't receive the email?

N.B. They have the option to turst the device for 30 days, to save doing this on each login should they wish.

If they chose an authentication app, then please see the steps below for using an authenticator app

Authenticator app

It will be mandatory for users to set up an 2FA via an authenticator app in order to log in. As soon as their email and password have been input, they will be presented with this screen:
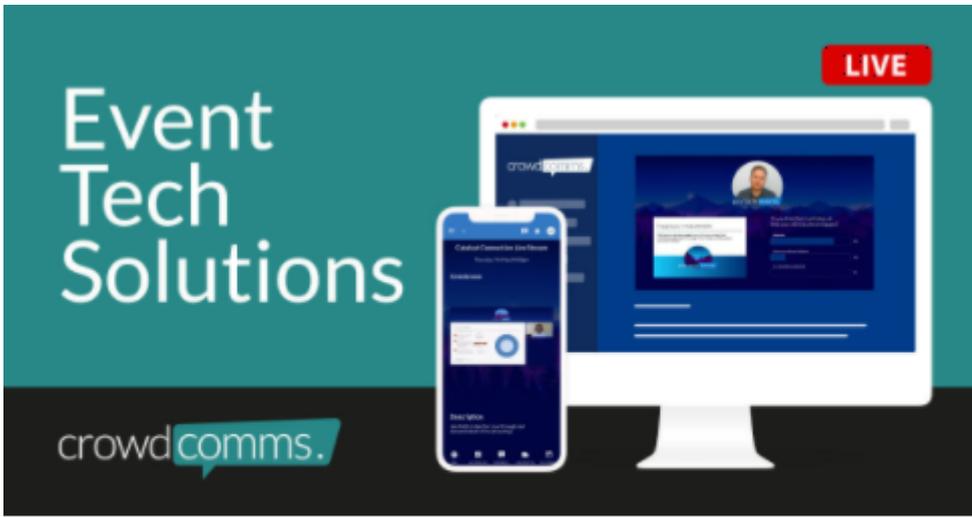
Set up 2-Factor Authentication

Use a 3rd-party authenticator app to improve the security of your account and prevent unauthorised access. Simply open your authenticator app and scan the QR Code below or enter the unique key into the app to continue.

Scan QR code using your app

OR

Enter this code in to your app

OLDEJCZI37MJR52I

CANCEL   NEXT

Once you have either scanned the QR code or entered the 16 digit number manually, you will then be provided with a 6 digit one time code to enter into the next screen on the App.

N.B. The 6 digit code is valid for 60 seconds (Your authenticator App will issue a new code after this time has expired)
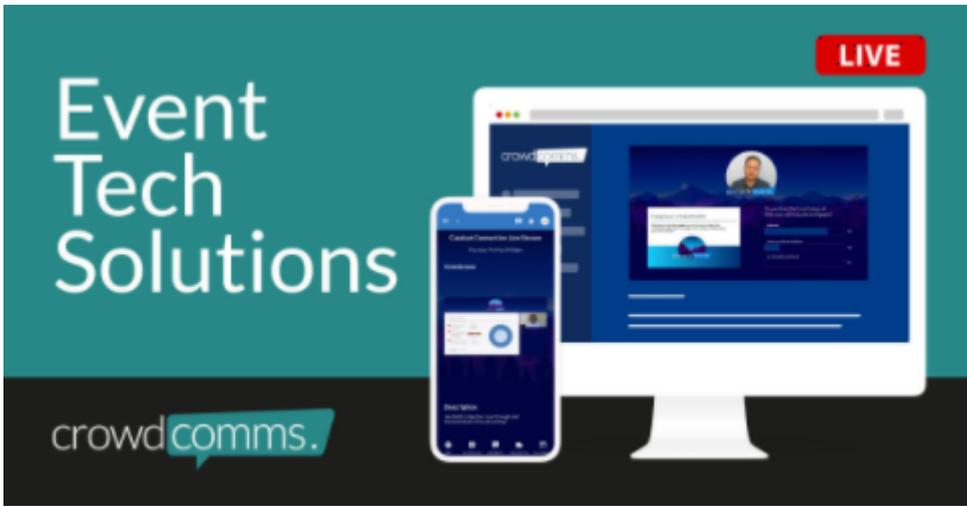
Authenticate device

Open your third party authenticator app and enter the 6-digit code below.

| 7 | 4 | 5 | 1 | 6 | 3 |

CANCEL   NEXT

As with email verification

Most people will be familiar with Authentication apps, but for anyoe who hasn't used oe before, you can point them in the direction of these common ones:

- *Authy*
- *Microsoft Authenticator*
- *Google Authentictor*
- *LastPass*
- *OTP*

Managing Your Devices

On the front end, you can have more than one device for authentication. To manage your devices you need to go to the top-right profile menu and click 'my account'.

There you can:

- Edit your device name

- Add or Remove a device
- View when a device was added to the account

Lost Devices

If a delegate loses their authentication device, they will need to contact you as the event organiser to reset it for them.

To do this, you just need to find their profile in the people library, and then scroll down all the way to the bottom and click 'reset authenticator devices'. This will remove the attached device from their account and allow them to set one up again from scratch.
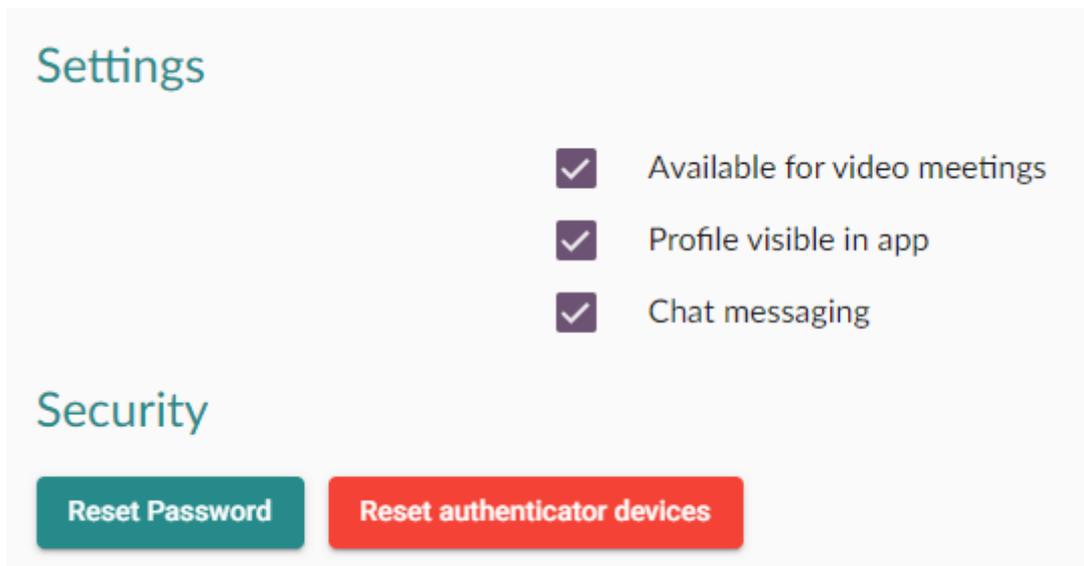
Please note:

- If a passcode has been added to your app, this comes after everything as the very last step.
- SSO overrides everything as it already requires verification via a third party

Revision #8
Created 9 July 2021 08:24:32 by Steven Slesser
Updated 19 August 2021 16:26:36