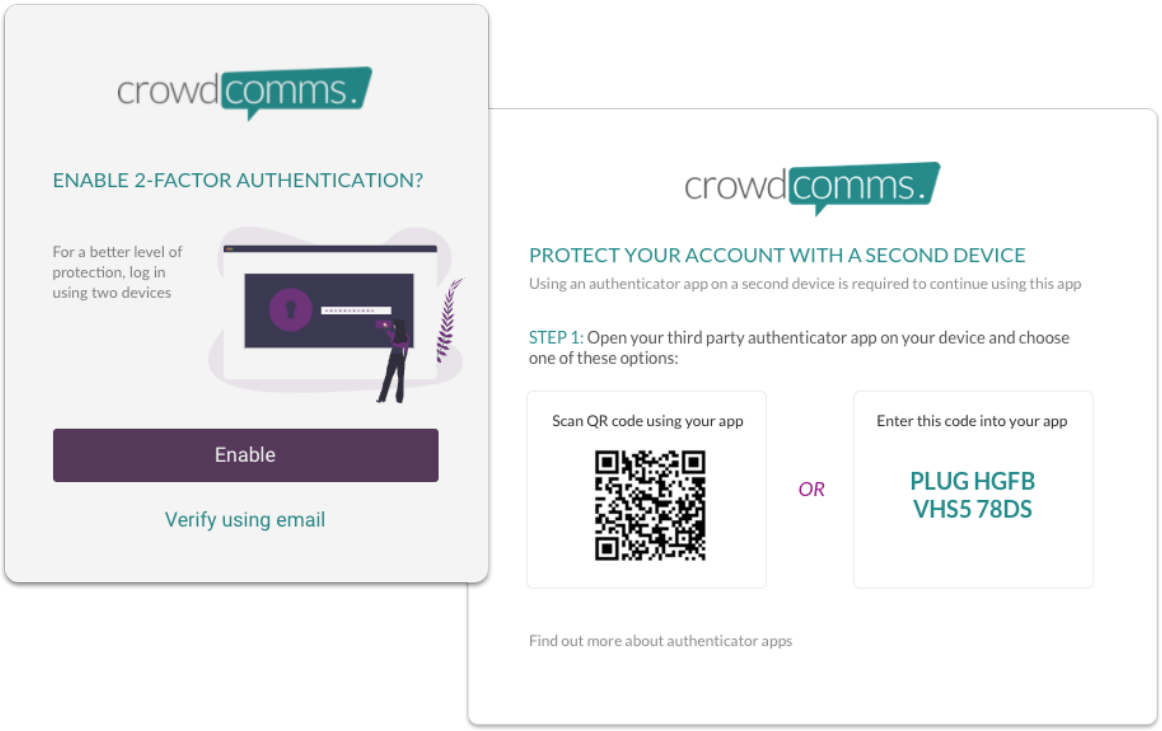
June Roundup: Security Upgrades

Two-factor Authentication. Extra security for your event

Click here to go to training guide

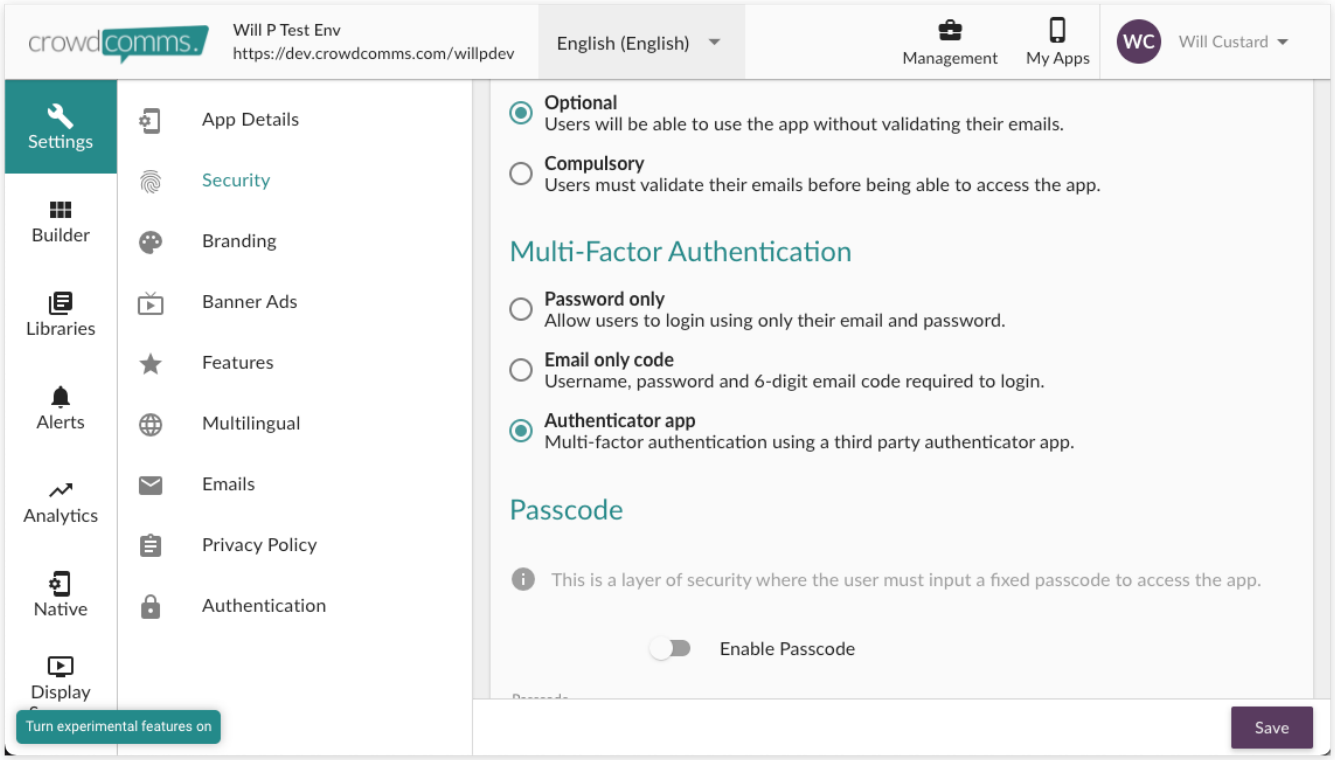


To keep your event as secure as possible we've now added the option of 2-factor authentication to your event apps. This is a great way to make sure user accounts cannot be compromised and gives you peace of mind that everything within the app is a safe as it could be.

Wondering what 2-factor authentication actually is? here's a definition:
Two-Factor Authentication (**2FA**) **works** by adding an additional layer of security to your online accounts. It requires an additional login credential – beyond just the username and password – to gain account access, and getting that second credential requires access to something that belongs to you.

We've got a few different options that you can use on your events so here's a

breakdown:



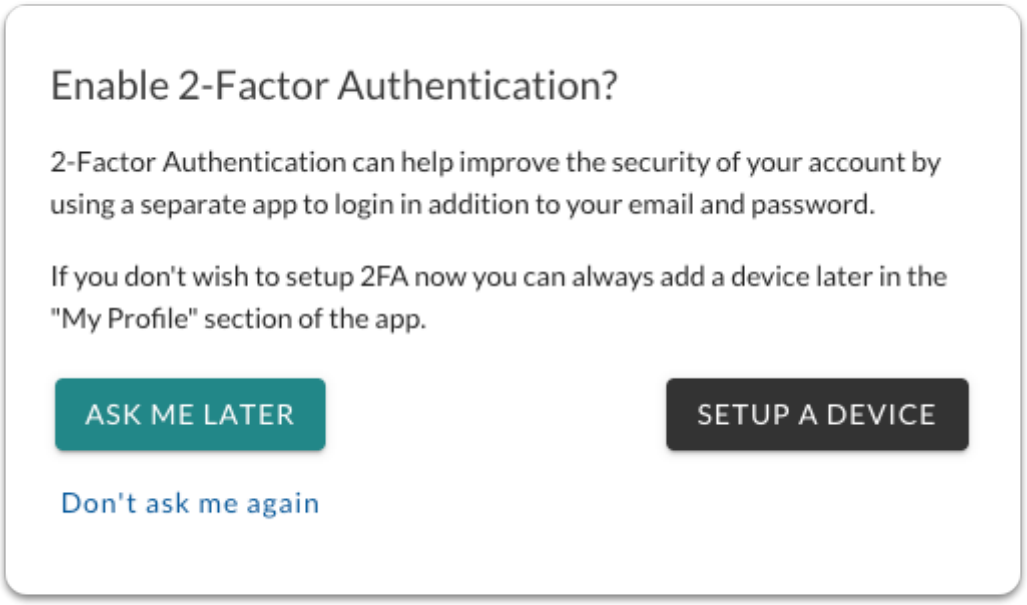
In the settings section of the Dashboard, within security you'll see a new section titled Multi-Factor Authentication.

From here you'll have 4 options

Continue without 2-Factor Authentication

One of your options will be to continue without 2-Factor Authentication enabled on your event. This is the least secure setting so won't be the default but we recognise that sometimes you won't want to interrupt the log in flow with an extra step.

Password Only

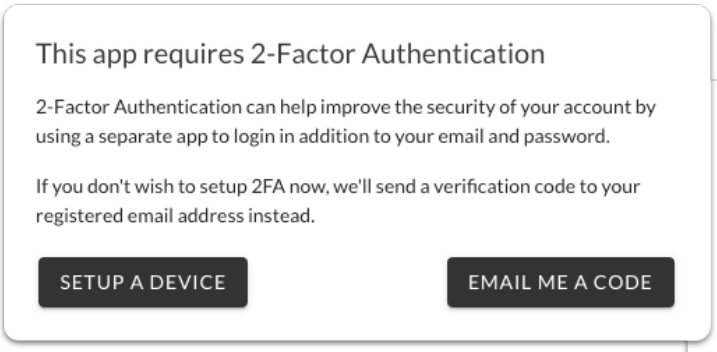


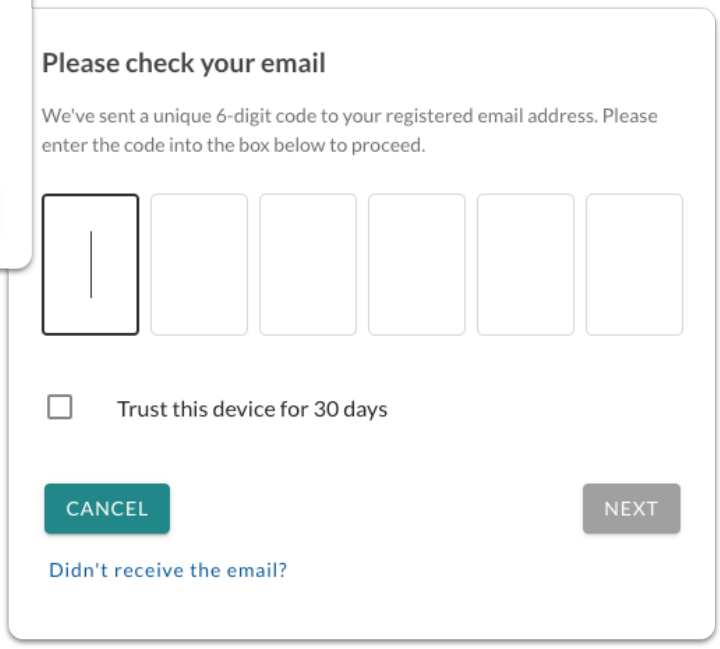
All events will obviously keep the username and password login steps.

'Optional 2FA' will mean that your event will ask your attendees to login into with their username and Password as usual, however, all users of the event app will be given the option to use 2-factor Authentication if they would like to. This can be dismissed in a couple of different ways. 'Ask me later' will allow users to continue to the app and ask them again next time they log in.

Clicking 'Don't ask me again' means that user will not see the prompt on this browser again unless they clear their storage.

Email Verification





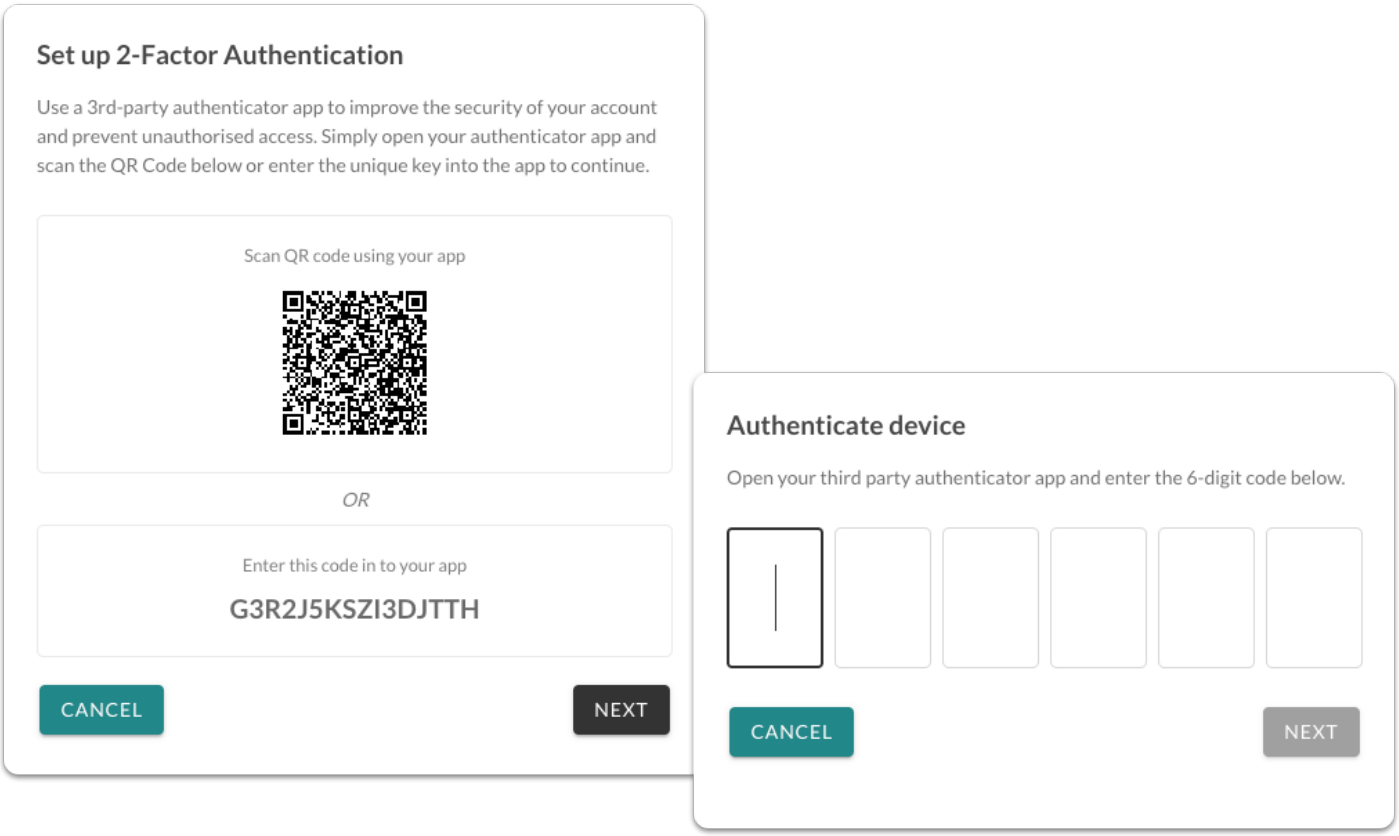
The 'Email Verification' option enforces a second factor on login for all app users. As a minimum, everyone logging in will need to retrieve a six digit code from their registered email address. This is

a great way to ensure your event is secure without the need for a second device to be present.

This setting is a great compromise between security and UX as it's solid way to protect your account but has a little less friction than having to use a second device.

As with the 'Optional 2FA' setting, users can choose to set up a second device if they wish to. By clikcing on 'Set up a Device' they will be able to scan a QR code or enter a pin into their third party authenticator app and log in with the peace of mind that their account is as secure as it possibly could be.

Authenticator App



Full, belt and braces 2-Factor Authentication will require all users to connect a second device to their account. It's a simple process which involves installing an authenticator app to their device and either scanning the QR code on screen or inputting the 16 digit code (sometimes referred to as a key).

The authenticator app will respond to our code with its own 6 digit code, which users will input into the site before being allowed into the event app. Once you've connected a device you'll be asked if you would like to remember the code for 30 days. This option will reduce the login time whilst keeping the high level of security in place.

We support all standard authenticator app but here's a few of the most common ones:

- Authy
- Microsoft Authenticator
- Google Authenticator

- LastPass
- OTP

Revision #7
Created 2 December 2021 14:23:48 by Lee Jack
Updated 6 February 2022 09:24:17 by Safia Sulani