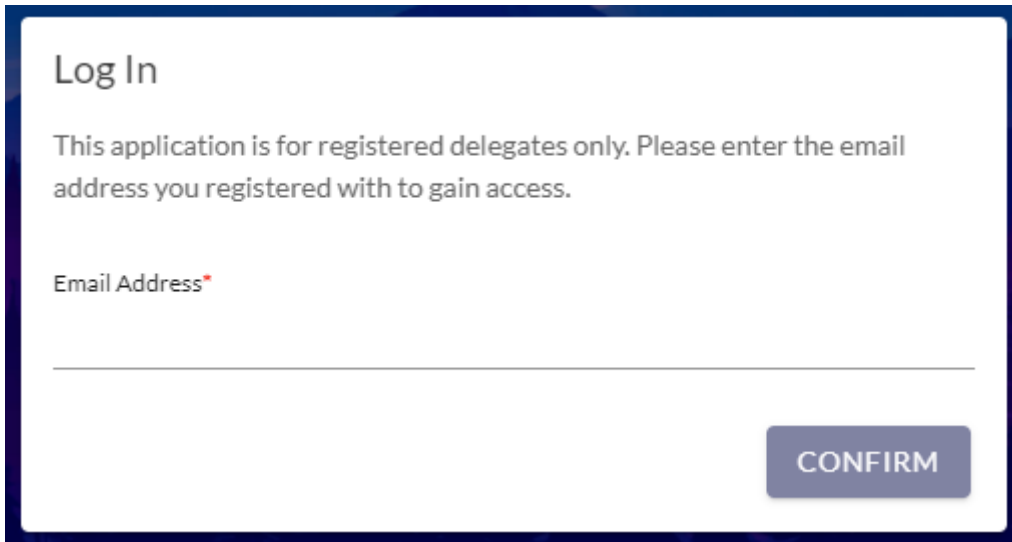


Mandatory 2FA

How to Log In

Step 1: Enter your email address

A screenshot of a login form with a dark blue border. The form has a title 'Log In' at the top left. Below the title is a message: 'This application is for registered delegates only. Please enter the email address you registered with to gain access.' Underneath this message is a label 'Email Address' followed by a red asterisk. Below the label is a horizontal input line. At the bottom right of the form is a grey button with the text 'CONFIRM' in white capital letters.

Log In

This application is for registered delegates only. Please enter the email address you registered with to gain access.

Email Address*

CONFIRM

N.B If this is your first time using our platform to access an event, then upon your first login you will then be presented with a mini reg form after entering your email.

Step 2: Fill out your details and create a password

Register

Email Address*

First Name*

Last Name*

Set your password

Your password must be 8 characters or more and contain at least 1 upper case, 1 lower case, 1 numeric, and 1 special character

Password*



Confirm Password*



CANCEL

REGISTER

N.B. For each subsequent login you will be taken straight to step 3.

Step 3: Enter your password

Welcome

Email Address*

Password*

Reset Password

CANCEL LOGIN

The login form is enclosed in a dark blue border. It features a 'Welcome' heading at the top. Below it are two input fields: 'Email Address*' and 'Password*'. The password field includes a small icon of a smartphone with a '5' and an eye icon for toggling visibility. To the right of the password field is a blue link that says 'Reset Password'. At the bottom of the form are two buttons: a purple 'CANCEL' button on the left and a dark blue 'LOGIN' button on the right.

N.B If at any point you forget your password, you can select the 'reset password' option which will send a link to your email allowing you to reset.

Step 4: Setting Up 2FA

You will be presented with the screen:

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

The screen has a dark blue border. It starts with the heading 'This app requires 2-Factor Authentication'. Below this is a paragraph explaining that 2FA improves account security by requiring a separate app. Another paragraph states that if the user doesn't want to set up 2FA now, a verification code will be sent to their registered email. At the bottom, there are two dark blue buttons: 'SETUP A DEVICE' on the left and 'EMAIL ME A CODE' on the right.

You have the option to either set up a device via an authentication app, or to receive a code via email.

Step 4: Option A – Setting up a Device

Once you click 'set up device' you will see the following 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

2PYO5HLSQJ6IWC4Q

CANCEL

NEXT

You can choose to either scan the QR code via your authentication app, or to manually enter the code.

If you are unfamiliar with authentication apps, then here are some familiar ones you may like to try:

- Google Authenticator
- Microsoft Authenticator
- Authy
- LastPass
- OTP

Once you have entered the code the app will be setup with your authentication device and will generate a 6-digit code that refreshes every 60 seconds.

Enter the code generated by your app and click next:

Authenticate device

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

CANCEL

NEXT

You will then be logged into the platform.

N.B. If you log out and back in again within 24 hours you will not be required to use your authentication app again to verify. Upon your first login after the 24 hour period is over, you will be asked to authenticate again, but you will also at this point be given the option to 'trust this device for 30 days'. If you choose to tick that box you won't have to authenticate for another 30 days.

Step 4: Option B – Receive an Email Code

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

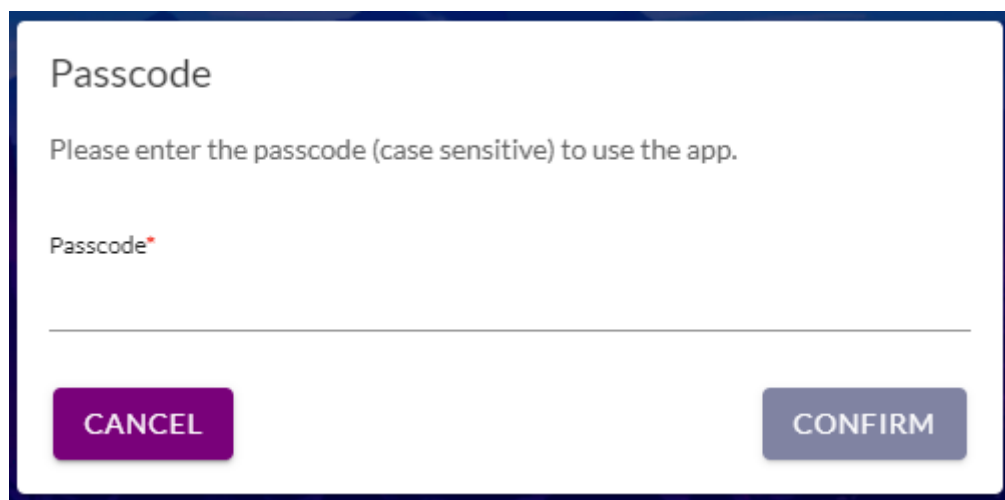
NEXT

[Didn't receive the email?](#)

Once you enter your 6-digit code and click next, you will then be logged into the platform. You also have the option to 'trust this device for 30 days', to save you having to authenticate each and every time you access the platform.

N.B. Your event organisers may have opted for one further required step and added a passcode to your event. If they have opted to do this, they will have provided you with a code that you will need to add directly onto the platform as the final step to log in.

Step 5: Enter your event passcode

A screenshot of a mobile app's passcode entry screen. The screen has a white background with a dark blue border. At the top, the word "Passcode" is written in a dark blue font. Below it, a grey instruction text says "Please enter the passcode (case sensitive) to use the app." Further down, the label "Passcode*" is shown in grey next to a long, thin, empty text input field. At the bottom of the screen, there are two buttons: a purple button on the left with the word "CANCEL" in white, and a grey button on the right with the word "CONFIRM" in white.

Managing Your Authentication Device

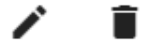
You can manage the device you have set up via your profile menu top right, at any point when logged into the platform.

To do this you need to go to 'My Account'. Here you can edit the name of your device to remind you which device you used if you find it helpful. You can also delete your device from here. If you delete your device, you will then be able to add another one to your account.

Account Settings

2-Factor Authentication Device

Device Name	Date Added
Device #1	7/13/21



If you delete and add a new device from here, you will then be taken through the same steps as before.

Lost Authentication Device

When you get to the authentication screen you have the option to select 'lost my authentication device'. You will then be prompted to contact your event organiser, so feel free to contact them directly without using this step. Your event organiser will then be able to reset the authentication device attached to your profile, allowing you to set a new one up from scratch again upon your next login.

Revision #1

Created 13 July 2021 18:04:37

Updated 19 August 2021 16:26:36