Using 2FA to access your CPD account.

AOA is increasing our cyber security to better protect members' data and privacy, as well as the Association's intellectual property by introducing two-factor authentication (2FA) for users of the new CPD system. 2FA is mandatory for all users of Salesforce-based platforms.

Users will have **three options** for logging into the training and CPD platform or app, Salesforce Authenticator, third-party authenticator apps, or built-in authenticators.

Most members will be familiar with 2FA, which is now commonly required for access to many business websites as well as online services including booking holidays, purchasing movie tickets, government services, banking, and accessing the AOA website.

2FA requires both of the following verification methods to access your account:

- something you know – which is your TIMS/CPD username and password.
- something you have – such as an authenticator app.

How to set up 2FA

When you log in to your CPD account, you will be prompted to provide an additional verification method.

1. Download your preferred authenticator app from the App Store or Google Play. (See options for authenticator apps below).
2. Log in to the CPD platform using your existing username and password at https://login.salesforce.com
3. Follow the prompts to choose a verification method.

Which authenticator app to use?

Authenticator apps work on the principle of providing a one-time identifier from a physical device, usually your mobile phone.

These apps are confirmed to work with the CPD platform and are available from the App Store or Google Play.

All users must register **at least one verification method** to connect to their training or CPD account. SMS (text message), phone call, and email verification are **not** supported.

Authenticator app	How it Works	URL
Option one: Salesforce	After a user enters their username and password, the app sends a notification to your mobile device. The user taps the notification to open Salesforce Authenticator which verifies the request and completes the login.	Apple App Store Google Play
Option two: Third-party authenticator apps • Google Authenticator • Microsoft Authenticator • Twllio Authy	During login the user is requested a code that is generated by this app as a one time password. These apps can be used without internet access.	Google Authenticator • Apple App Store • Google Play Microsoft Authenticator • Apple App Store • Google Play Authy • Apple App Store • Google Play
Option three: Built-in authenticators • Windows Hello • Touch ID Face ID	Built-in authenticators verify a user's identity through a biometric reader, which is built into a users computer or mobile device. After you enter a username and password, the built-in authenticator prompts you for a biometric (fingerprint, iris, or facial recognition scan), PIN, or password identifier. NB: Built-in authenticators can't be used for MFA verification in the CPD mobile app. To log in to the mobile app, users must register a backup verification method such as an authenticator app in options one or two above	

How to connect to an authenticator app

A set of instructions are linked below for each authenticator app option.

Option one: Salesforce
Option two: third-party authenticator (Google, Microsoft, or Twilio)
Option three: built-in authenticators

Further support

Should you require assistance, please contact AOA IT support at ithelp@aoa.org.au