About Multi-Factor Authentication

Overview

- Multi-factor authentication (MFA) adds another layer of security to your ClickSuper account.
- When you log in to ClickSuper, enter your username and password, then enter the authentication code.

About multi-factor authentication

What you need to know

We understand that keeping your information secure by preventing unauthorised access is important to your business.

Multi-factor authentication (MFA) provides an extra level of security and is one of the best steps you can take to keep your ClickSuper account safe. This makes it much harder for someone else to impersonate you and gain access to your ClickSuper account.

MFA is mandatory for all users of ClickSuper to support the ATO's requirements for digital service providers (DSPs).

After entering your username and password, you generate a code using the Google Authenticator app on your mobile device, then enter the code in ClickSuper.

- If you access more than one organisation under the same login, you only need to set up MFA once, as it applies to any device or browser you use to access ClickSuper.
- If you access different organisations using different logins, set up separate MFA accounts for each login, using the same Google Authenticator app.
- No one else can log into your account, as you're the only one who knows your username and password and has access to your authentication device.
- If you use the same computer and browser each time you log into ClickSuper, you can choose a number of days to remember the authentication code instead of entering it every time you log in.

MFA using the Google Authenticator app

If you already use the Google Authenticator app, add another account to it for your ClickSuper login.

If you don't have it installed already, you can download it from Apple App Store (for iPhone) or from Google Play Store (for Android)

How it works

Although you use Google Authenticator to generate the codes, the app doesn't connect to your ClickSuper organisation(s) and there's no transfer of data between them.

- The app automatically generates new codes each time you open the app, and doesn’t need a network connection or mobile signal to do this.
- ClickSuper generates the same codes, so when you enter the code from your app, it matches ClickSuper, verifying it's you logging in. Both codes are generated using the same secret key that's unique to you. No two ClickSuper accounts generate the same code.
- When you set up MFA, enter the key into your app by scanning a QR code or entering it manually.

The codes are time-based, so make sure the time on your authenticator device is in sync with ClickSuper. Let your network provider set the time automatically on your device to prevent getting an out-of-sync or invalid code error.

Alternative MFA options

If you do not have access to a phone, you can install the Unofficial (open source) Authenticator Chrome Extension here: https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai?hl=en which enables you to generate your MFA code using your Chrome web browser

If you don't have access to your authentication device for any reason, you can log in using the answer to your security question.

It’s mandatory to set up a security question and answer during the MFA set up.