Guide for using two-factor authentication (2FA)

Q-global™ User's Guide

May 2018

Pearson

Guide to using two-factor authentication (2FA)

Two-factor authentication (2FA) is a complement to your username and password, which further increases the protection of your account on Q-global™. When you log in with two-factor authentication (2FA), in addition to username and password, you will be given a one-time password that you alone have access to. Combining usernames, passwords and one-time codes makes it much more difficult for unauthorized people to access your data.

Pearson has introduced two-factor authentication on Q-global to meet the requirements of the new privacy regulation GDPR (General Data Protection Regulation).

You have probably already come into contact with two-factor authentication (2FA) through other services such as internet banking, social media and other applications.

Steps to set up 2FA on Q-global:

1. The first time you log in to Q-global before 2FA has been activated, you will see a window explaining what 2FA is. You cannot continue until you have configured at least one authentication method
2. Click **"Enter 2FA details"** to continue
3. You can set up three different methods for 2FA: **Google Authenticator**, **SMS (text message)**, or **email**. For instructions on how to set up each of these methods, **see page 3**
4. Once you have set up one or multiple methods for 2FA, you will be prompted to use 2FA next time you login. Enter your login details as usual. If you have set up multiple methods, you will be able to choose between the methods you set up. For example, you can choose to receive the code via email or use Google Authenticator (depending on the methods you have set up)
5. Enter the code from Google Authenticator or the one you receive via SMS or email
6. Click **"Login"**.

For more information, visit pearsonclinical.co.uk/q-global

Pearson

Instructions for Google Authenticator 2FA:

Google Authenticator is a free app which can be downloaded on most smartphones. The app generates single-use codes that can be used to verify login on different websites and applications. Google Authenticator is easy to use and works without internet connection. The application generates a new code every 30 seconds, and is therefore a very secure method for 2FA.

1. To enable Google Authenticator, first you must download the app. Search for **"Google Authenticator"** in the App Store, Google Play, BlackBerry World or Microsoft Store depending on whether you have iPhone, Android, BlackBerry or Windows Phone
2. Once Google Authenticator is installed on your phone, open the app and **click the plus sign**
3. Select **"Read barcode"** and allow the app to access your phone's camera
4. Click on **"Configure GA"** on the Q-global™ 2FA setup page
5. **Scan the QR Code** with your mobile phone. A six digit code should appear on the phone
6. **Enter the 6 digit code** on the top right into Q-global and click **"Confirm"**. A green check mark should appear to confirm that the code has been verified
7. Click **"Submit"**
8. You can now click **"Home"** at the top left to go to the Q-global overview page
9. Google Authenticator is now enabled in your account and you must enter a six-digit number from the application when you log in. 2FA is valid for 12 hours on the same computer. 2FA via SMS or email is configured in the same way.

Instructions for SMS or email 2FA:

1. **Enter e-mail address or mobile phone number** and click **"Confirm"**. A one-time code will be sent to your email or phone, depending on the method you selected
2. **Enter the code in the box** below and click **"Confirm"**. A green box verifies that the configuration process is complete
3. Click **"Submit"** in the top right corner to save your changes.

For more information, visit pearsonclinical.co.uk/q-global

Pearson