Standard Life
Part of Phoenix Group

Multi Factor Authentication (MFA) – setup guide

Introduction

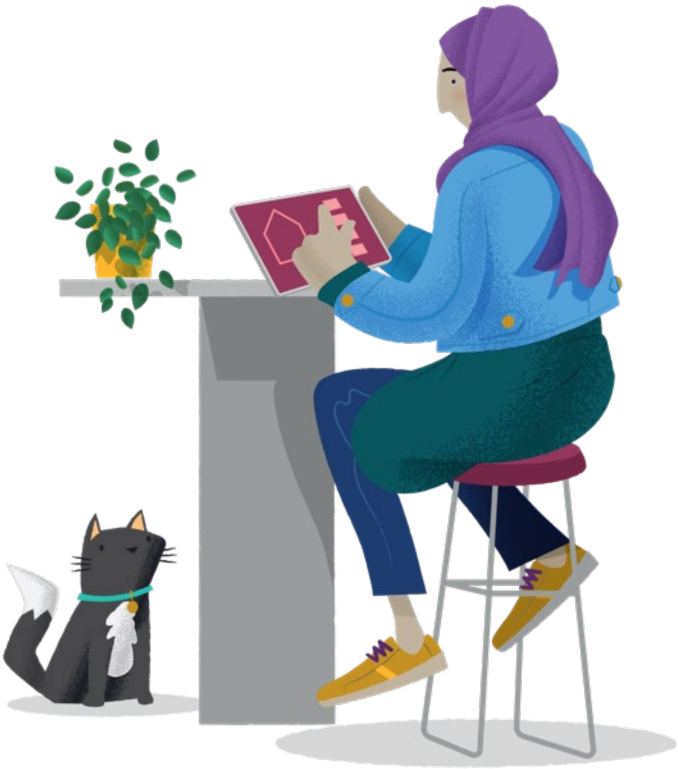
We're introducing multi-factor authentication to our workplace administration platforms.

As an administrator of your scheme on the Standard Life workplace administration platform, you'll be required to set up multi-factor authentication using an authenticator app before accessing the platform. Multi-factor authentication is designed to keep user access secure and add an additional security step when logging in.

You'll still use your exisiting username and password but will now be asked to enter a security code from your chosen authenticator app. There are many apps available that can be used but the recommended apps would be Google authenticator or Microsoft authenticator.

Setting up multi-factor authentication is simple and we've documented the process required in this guide.

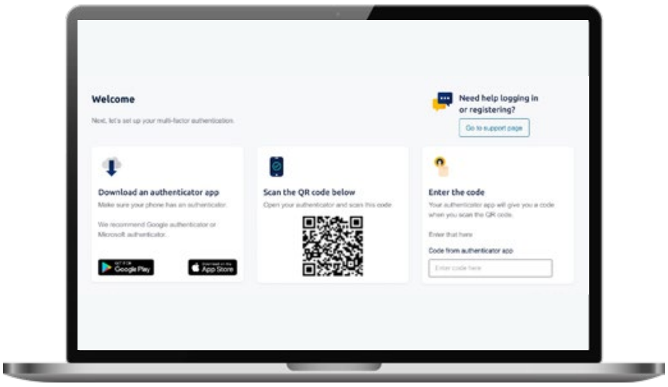
You'll not be able to log in without completing this process.



Setting up multi-factor authentication

Logging in for the first time

Having entered your username and password as normal, you'll be presented with the following screen.



Welcome

Next, let's set up your multi-factor authentication.

Need help logging in or registering?

Go to support page

Download an authenticator app

Make sure your phone has an authenticator.

We recommend Google authenticator or Microsoft authenticator.

Google Play | App Store

Scan the QR code below

Open your authenticator and scan this code.

Enter the code

Your authenticator app will give you a code when you scan the QR code.

Enter that here

Code from authenticator app

Enter code here

You'll need to install an authenticator app on your mobile phone.

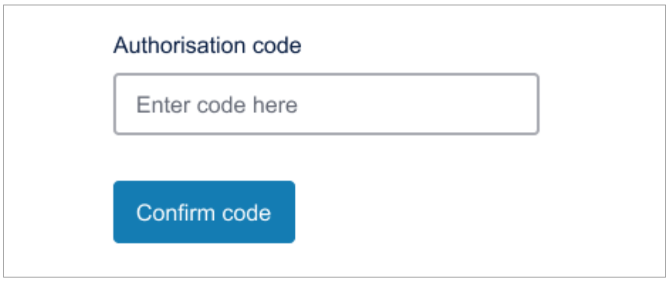
The authenticator app will allow you to set up an account by scanning the QR code or by manually entering the secret key supplied.

Once the account is set up on the authenticator app, it will generate a 6 digit one time password that you must enter.

You'll then be allowed on to the platform as normal.

Logging in when you have already set up multi-factor authentication

Having entered your username and password as normal on your administration platform, you'll be presented with the following screen.



Authorisation code

Enter code here

Confirm code

A 6 digit one time password will be generated by your authenticator app, this will happen each time you log in. Enter the code and click confirm code.

You'll then be allowed into the application as normal.

FAQs

What is multi-factor authentication?

Multi-factor authentication (MFA) is an authentication method that requires you to provide one or more verification factors to gain access to a resource, in addition to your usual username and password. MFA requires one or more additional verification factors, which increases the security on your account.

MFA requires you to set up an authenticator app (typically on a mobile phone) the first time you log in, and then enter a one-time password generated by that authenticator app. Subsequent log in attempts will require your username and password followed by a new one time password generated by your authenticator app.

What authenticator apps are available?

The technology that supports this kind of MFA is open source and standards based. This means that there are many different applications available for different platforms, all achieving the same result. It is up to you on which app is chosen however, the two most popular are Microsoft Authenticator and Google Authenticator; both are available for Android and IOS devices.

What is a trusted device?

A trusted device is typically a mobile phone or tablet that is registered on the authenticator application.

What is a secret key?

The secret key is a unique alphanumeric code which is shared between the workplace administration platform and an authenticator app. It allows the authenticator app to generate a one-time password for the user to enter; and the platform to generate the same one-time password to validate the value entered by the user. It is usually imbedded in a QR code that can be read by a phone or manually inputted.

What is a one-time password?

A six-digit number, generated by an authenticator app that is valid only once and only for a limited period of time.

What should I do if I lose or "factory reset" my trusted device?

You cannot access the platform without using your trusted device authenticator app. If you forget, lose or use factory reset on your trusted device please call our helpdesk on 0345 60 60 092. We can reset MFA and allow you to restart the process on your new or reset device after reinstalling the authenticator app. You may also have to delete the original account from your device and replace it with the account generated from the new QR code.

Is there any charge for implementing MFA?

There is no charge for this.

Can I use my email address rather than my mobile phone number?

Using email for passcodes doesn't qualify as multi-factor authentication as there is only one factor for both user id/password and email/password to access emails. Solutions which use passcodes sent to email are technically described as two-step verification rather than multi-factor authentication. From a security perspective two-step verification is known to be less secure than MFA and at higher risk of being compromised.

Can I add new/additional user?

MFA is required for every unique user – it is not possible to share this functionality or log in access. If you would like to set up a new authorised user of the workplace administration platform, please follow the **usual registration process**. MFA set up now forms part of registration.

Please ensure your companies authorised approver is aware a registration email will be sent and require approval from them.

Standard Life Assurance Limited is registered in Scotland (SC286833) at Standard Life House, 30 Lothian Road, Edinburgh EH1 2DH.

Standard Life Assurance Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. **www.standardlife.co.uk**