First Briefing, October 2023 – Client Hub security update

Multi-factor authentication (MFA) has been available on our Client Hub for some time, but only as an optional feature.

To make the data of all our clients as secure as possible, MFA will become mandatory on our Client Hub from 31 March 2024.

Why are we making this change?

MFA significantly improves your digital security by requiring multiple forms of verification to access online accounts. So even if your password is compromised, an attacker would still need another factor, such as a mobile device, to gain access.

Many First Actuarial clients are already using MFA on the Client Hub. Even if you aren’t, you’re probably familiar with the concept through online banking or common internet logins like Google and Microsoft.

We will be strengthening security for all our clients by requiring the use of MFA from 31 March 2024. By notifying you well in advance, we’re giving you every chance to find out what it means and how it will work before we make the change.

How effective is MFA?

Microsoft has stated implementing MFA is the…

> “one simple action you can take to prevent 99.9 percent of attacks on your accounts”

A similar study by Google in 2019 noted that MFA using an SMS code…

> “helped block 100% of automated bots, 96% of bulk phishing attacks, and 76% of targeted attacks”

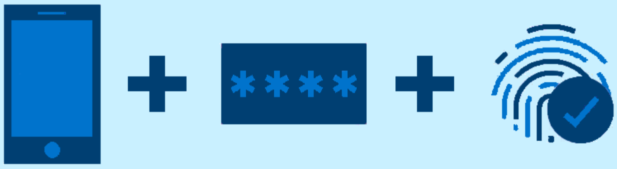
Unfortunately, hackers don’t stand still, and those figures – for targeted attacks at least – are likely to have fallen slightly since 2019. Even so, the benefits of implementing MFA should be clear.

What is MFA exactly?

MFA is a security mechanism that mandates users to provide two or more distinct forms of identification before gaining access to an account or system. The primary aim of MFA is to enhance security beyond the conventional username and password, significantly reducing the risk of unauthorised access.

MFA usually requires you to provide two or more of:

- **Something you know:** A traditional password or personal identification number (PIN)
- **Something you have:** A tangible object like a smartphone or a smart card, or a security token
- **Something you are:** Biometric data, such as fingerprints, facial recognition or voice recognition.



You can enable MFA in a number of ways. For example, you may receive a one-time code via a text message, or use a mobile app (like Google Authenticator) or biometric scans. By requiring multiple forms of verification, MFA provides a robust defence against unauthorised access attempts, even when your password has been compromised.

The information contained in this bulletin is, to the best of our knowledge and belief, correct at the time of writing. However, First Actuarial cannot be held liable for any errors contained herein and the recipient accepts that the information stated is provided on an "as is" basis. This briefing is for general information only. It does not and is not intended to constitute advice. Specific advice should always be sought from the appropriate professional on all individual cases.

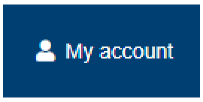
Regulated in the UK by the Institute and Faculty of Actuaries in respect of a range of investment business activities.

First Actuarial LLP is a limited liability partnership registered in England & Wales. Number OC348086.

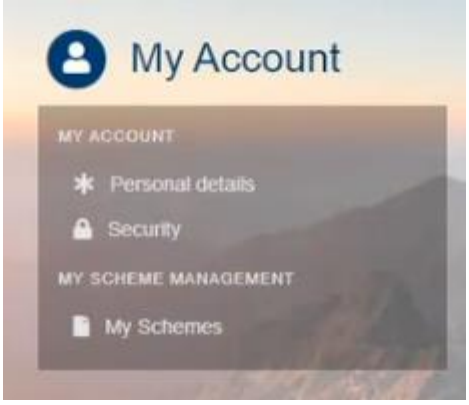
Registered address: First Actuarial LLP, Mayesbrook House, Lawnswood Business Park, Leeds, LS16 6QY

Can I implement MFA on the Client Hub sooner than March 2024?

Yes. You can switch on MFA now from the ‘My account’ link at the top right of any Client Hub page.



Once here, select the Security option on the left-hand menu.



Here you can enable MFA for your own account.

If you’d like to go further and require MFA for anyone who has access to your scheme information on the Client Hub, please speak to your usual First Actuarial consultant who will switch it on for you.

What options are there for the second factor and how can I change them?

We currently allow you to use one of the following:

- Email
- SMS text message
- An app like the Microsoft or Google authenticator apps (known as a TOTP app).

However, please note that using email is significantly less secure than the other methods. For this reason, we strongly recommend that you avoid using it and set up SMS or a TOTP app instead. This is because if your account is compromised, there is a reasonable chance that your email is compromised as well.

You can manage these options under the Security page in the My Account area, as set out above.

Watch our video to learn what to expect when MFA is enabled and how to change your options.

What else is useful to know about MFA?

Implementing MFA doesn’t guarantee that your account will never be compromised. But by following a few simple rules, you can minimise the risk of having your credentials stolen:

- Never share your MFA security codes with anybody else.
- Be suspicious if you get a message (by email, SMS, Teams etc.) that you aren’t expecting or that looks unusual (e.g. typos, unfamiliar subject matter, or just a tone that feels ‘off’). This also applies to phone calls – especially with the rise in voice-cloning technology.
- Be even more wary if the message suggests opening an attachment, clicking on a link or making a financial transaction. Make every attempt to work out whether the message is legitimate before taking any action.
- Check that all links look like they’re going where you are expecting. If you can, take the time to learn about links – their structure and which bits are important to check.

Further information

For further information, or for trustee training on cyber security, please contact your usual First Actuarial consultant or our Head of IT.

Mark Rowlinson FIA MBCS
Partner/Head of IT
E: mark.rowlinson@firstactuarial.co.uk
T: 07813 852748