

CMA Bulletin

To: CMA MEMBERS
No: BU179
Title: Multi-Factor Authentication for Cloud Systems
Purpose: For Information
Expiry date: 1 September 2026
From: Amanda Hancock
Date: 18 August 2026

This Bulletin is to inform Market Participants that we are enabling multi-factor authentication (MFA) for access to our cloud systems. MFA adds an extra layer of protection by asking users to confirm their identity using a second method, such as approving a notification in the Microsoft Authenticator app, entering a one-time code, or using another approved verification method.

This change is being introduced to strengthen the security of company data and cloud services, reduce the risk of unauthorised access, and support our Cyber Essentials obligations. MFA is particularly important because a password on its own may not be enough if it is guessed, reused, or exposed elsewhere.

When you sign in to cloud services such as Microsoft 365, Teams, SharePoint, or other connected cloud applications, e.g. for Technical Panel paper access or Market Audit / PoLR file submission and viewing purposes) you may be prompted to complete an additional verification step after entering your password.

The preferred method is to use the Microsoft Authenticator app, which can send a notification to your mobile device for approval. Currently available alternative approved methods may include a one-time code, SMS, or voice call where these are available and appropriate. However, Microsoft is planning to retire the options for SMS and voice call so these are not recommended.

This already applies to CMA employees, and we are now extending this to authorised users who access CMA cloud systems. Some guest users or specific accounts may be handled separately where an exclusion or phased approach is required, but the general expectation is that MFA will be used wherever it is supported.

MFA will be enabled from **31/08/2026**. After this point, guest and external users may be asked to register their verification method the next time they sign in to a cloud service.

What do I need to do next:

1. Download the Microsoft Authenticator app from your mobile device's app store, if you do not already have it.
2. When prompted during sign-in, follow the on-screen instructions to add your work account.
3. Choose your preferred verification method. We recommend app notifications where possible.
4. Complete the test verification to confirm the setup has worked.

The first-time setup should only take a few minutes. Once configured, MFA prompts are straightforward and will usually only appear when needed, such as when signing in from a new device, location, or browser.

If you have any issues setting up MFA, do not have access to a suitable device, or believe you may need an alternative verification method, please contact Enquiries@cmascotland.co.uk as soon as possible. Thank you for your cooperation in helping keep CMA systems and Market data secure.

Regards,

Amanda

CentralMarketAgency

Stakeholder Manager

48 Enterprise House, Springkerse Business Park, Stirling, FK7 7UF

t 01786 468871 | m 07770 926 438

e amanda.hancock@cmascotland.co.uk | w www.cmascotland.co.uk