Portal User Guidelines:
Security upgrade to the Portal - MFA emails

Status	Version 1.0
Date	April 2024
Document owner	CPL
Document author	Ali Gibbs
Document purpose	The purpose of this document is to provide guidance for Administrators on handling duplicated MFA email addresses in Production.

Contents

1. Introduction for Administrators

In the upgraded Portal, a **UNIQUE** MFA email address is mandatory for all users wanting to access the web services:

- Admin console (e.g. Administrators)
- The portal web site (e.g. claim handlers)
- Users who need access to Archived claims and
- Users who need to delete claims
- Users in Training
- Web users in a2a Test

The unique MFA email address is also required for the user to obtain their personal password in a secure way and reset, when necessary. **As an Administrator, it's very important for you to review your user accounts and make any necessary changes in the way described, in order to retain access the Web services.**

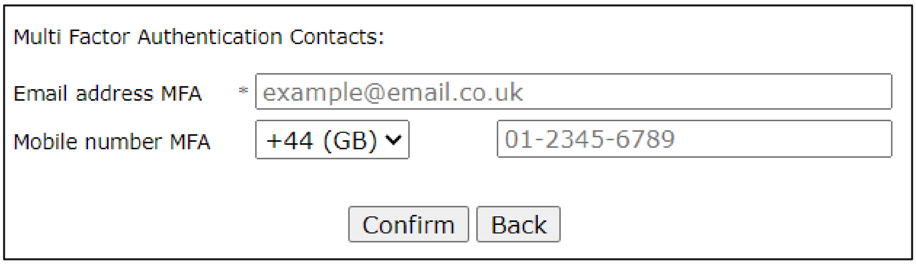
The MFA email address must be **UNIQUE** within your Organisation but can be used multiple times within different Organisation ID(s). See table below:

	Description	Outcome	Action
1	An individual, having several users with the same MFA email in **different** Organisations.	Will be possibile.	**No action needed,** on the basis that the individual is the same user acting on behalf of several Organisations.
2	Multiple users sharing same email within the **same** Organisation.	Will not be possible.	User must enter a unique email address.
3	An individual, having several user accounts with different profiles, within the **same** Organisation.	Will not be possible.	User can use the multi-profile function by merging the profiles into the same user account or enter a unique email address for each user account.

2. Guidelines to ensure you are ready for the Upgraded Portal - ADMIN ONLY

You need to ensure that the following information is correct and if necessary, update your profile and those of your users. Login to the Admin console, click on “User” and look up your UserID, click on “Edit”, check and update the following information:

- Personal information: The account must be personal to the user and include their First Name and Surname.
- MFA information: Email address is mandatory, and must be unique within your Organisation. Mobile number is optional. These are shown in the “Multi Factor Authentication Contacts” box that is visible, see below:

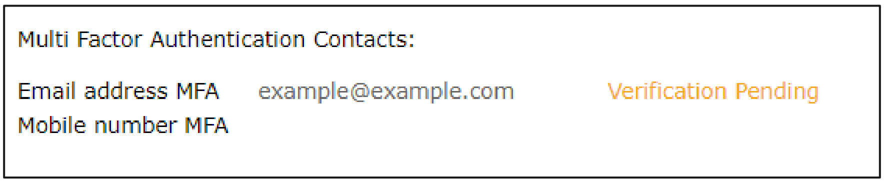


Multi Factor Authentication Contacts:

Email address MFA * example@email.co.uk

Mobile number MFA +44 (GB) 01-2345-6789

- Upon clicking on “Confirm”, all the information entered is saved and the box will appear as follows:



Multi Factor Authentication Contacts:

Email address MFA example@example.com Verification Pending

Mobile number MFA

- If the user is a new MFA user, the “Verification Pending” warning means they will receive an email from the Portal, containing a unique link that they need to click on within the next 24hrs and complete their email verification procedure. If they do not complete the verification procedure within 24hrs, the link will expire and you must request a new MFA token on their behalf.

The “Mobile number MFA” is optional, however when available, it is useful for you to complete your profile and fill in this information as it is an alternative way to request the MFA token.

As an Administrator you must check your list of users within your Organisation and identify those that are generic and do not contain an individual’s forename and surname and those that have the same MFA email address set. You must edit each user’s account, add the user’s forename and surname and set a unique MFA email address for every user/UserID.

3. What if the User has more than one account with the same email address?

An example would be when the user has multiple user accounts within the same organisation with different profiles.

The MFA email address is mandatory, and the admin console will not allow the MFA email field to remain blank, the following must be applied.

The Administrator must:

- Choose the user with the UserID you consider has the highest priority. This should be a Claim Handler account as it will be linked to the claims the user is managing.
- Make sure that the MFA unique email address is set.
- Convert the user account to a Multi-profile account by assigning to this user the profiles assigned to their other user accounts where the same duplicated MFA email address is present, so that the user does not lose operability.
- Make sure that there are no claims allocated to the old user account(s) or locked by the user to their old user accounts.
- Remind your Team Leaders to periodically check whether there are claims sent back to their organisation that were previously allocated to a specific user.
- Review the Web Site for guidance on User profiles: https://www.claimsportal.org.uk/administrator/profiles/

4. What's happening to users with duplicated email address when we migrate to the upgraded portal?

When users are migrated, in the event that you have users with the same duplicated MFA email within the same organisation, these users will be migrated without the email address and they will not have access to the Upgraded Portal until you update the information as described above.