CPL CFF Web

User guide for first access, password reset and login

|  |  |
| --- | --- |
| Status | Version 1 |
| Date | May 2024 |
| Document owner | CPL |
| Document author | Ali Gibbs |
|  | |
| Document purpose | The purpose of this document is to provide guidance for users on accessing the replatformed Web Portal, following the Go Live on 28th May 2024. |

# **Contents**

1 First login or reset password procedure….……………………………………………………….……………………… 2

2 Logging into the Portal…………………………………………………………………………….……….…………………….. 7

3 Possible error scenarios………………………………………………………………………………………………………….. 9

1. First login or reset password procedure

The first access and the reset password procedure for the new Portal Web service follow the rules of authentication used for Multi Factor Authentication.

The procedure for the first login and resetting/changing the password are the same. The procedure is the same for all the environments: Training/Integration and Production.

To perform the first login to the portal, the user must select the “LOGIN TO PORTAL” button on the homepage.

The user is required to have an account with an associated unique MFA email.

1. The user must login into the portal via the button below:

A screenshot of a web page

Description automatically generated

1. After pressing the button, the user will be taken to the page below where they can login for the first time or use “Forgot your password? Or Login?”.

A screenshot of a login screen

Description automatically generated

1. A new page will appear, and the user needs to enter their username and the MFA email associated to their account.  
   **Please note**: For migrated accounts, the username (sign in name) and the MFA email must be the same as the one used in the old environments (for both Integration and Production).

A screenshot of a login form

Description automatically generated

1. Press “Send Verification Code”. This will send the OTP for the first access, to the email associated with the user’s account, A confirmation message appears.

A screenshot of a cell phone

Description automatically generated

1. Insert the OTP code received via email and then click on “Verify Code”. Using “Send New Code”, the user can receive a new code for the account verification.
2. After verifying the OTP, a confirmation message appears and the user can then press “Continue”.

A screenshot of a computer

Description automatically generated

1. Press “Continue”, and a new view appears in order to set the password. The user can now set their password and click “Continue”. If the password meets the password validation rules, the account is then configured for future logins.

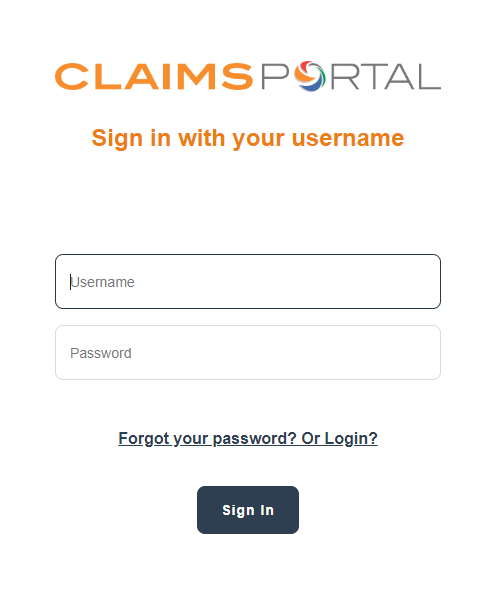
A screenshot of a login screen

Description automatically generated

1. Logging into the Portal

**Note**: After the first login, the user will be directed to step 2 for subsequent logins and the first part of the procedure is skipped.

For the standard login procedure, after pressing the “Login to portal” button in the homepage, the login view will appear:



1. The user can just type in their username and password and press the “Sign In” button. If the credentials are correct, a new window appears:

A screenshot of a computer

Description automatically generated

1. The user can choose whether to use email or their mobile number (if the user has been setup to receive the token on their mobile). By clicking on continue, a new window appears:

A screenshot of a login box

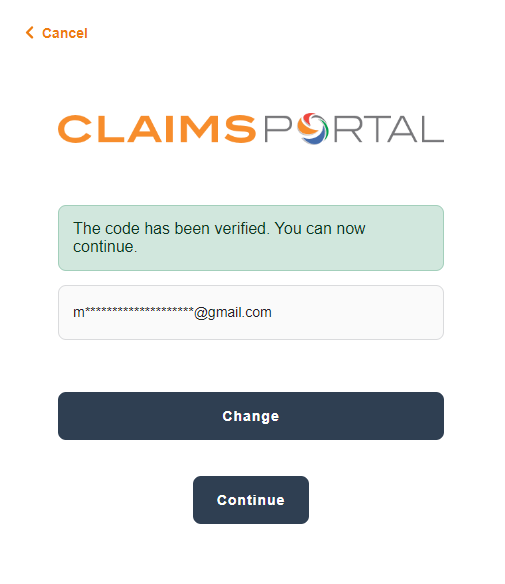
Description automatically generated

1. The user must click-on “Send Verification Code” in order to receive the code to log into the portal. When pressing this button, the OTP window will appear:

A screenshot of a phone

Description automatically generated

1. The user can type in the OTP received via email (or mobile) and can press “Verify code”, or “Send new code” in order to get another OTP.  
   After this, a new window appears that confirms the successful verification of the code:



1. The confirmation message means the user can select “Continue” in order to log into the portal.
2. Possible errors scenarios

3.1 Numbers of tries to authenticate allowed

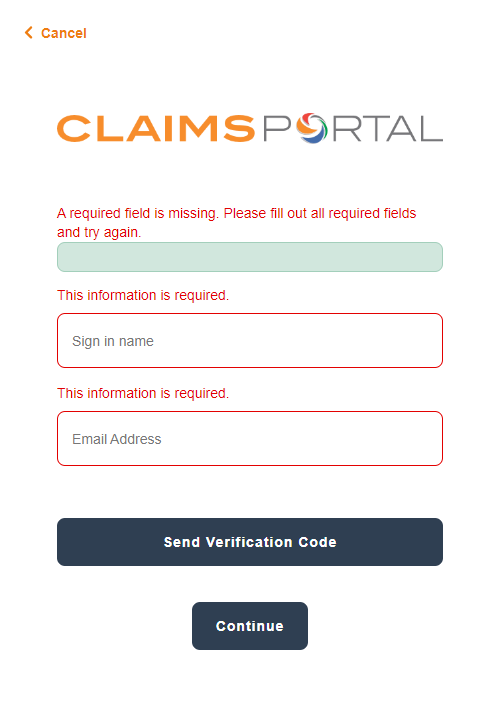
The new login allows the user a number of attempts before the systems blocks the user for a specific time.

* For the actual login with the password, the user has 10 attempts to enter the correct password; after the 10th attempt, further attempts blocked for 1 minute.
* Subsequent incorrect attempts will result in the blockage happening every time the user tries to log in and the time to wait is increased every 10 attempts that the password is entered incorrectly, up to a maximum of 5 hours.
* For the OTP, the system generates a token that can be entered a maximum of 5 times, after 5 attempts, the user must wait 10 minutes to generate a new code that can be used again 5 times.

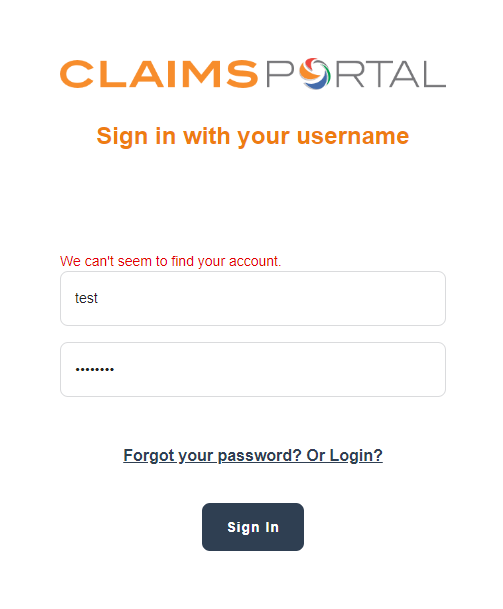
Both these cases generate error messages, displayed to the user in the login page.

3.2 Error messages

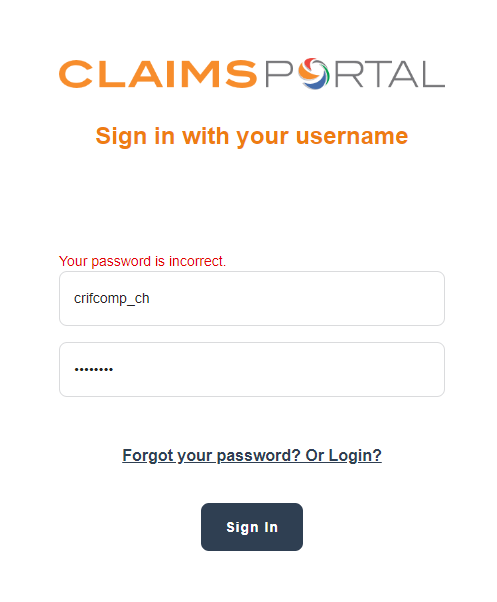
Generic required field messages; mean that a field that is necessary to login not entered



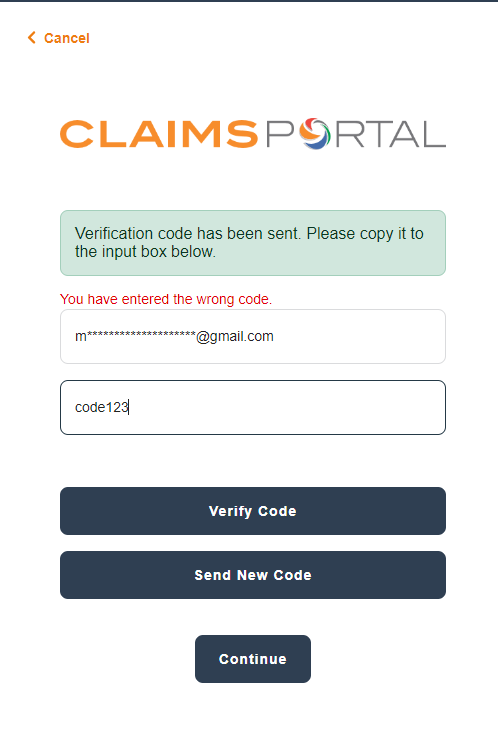
“We can’t seem to find your account”, means the username entered by the user does not exist.



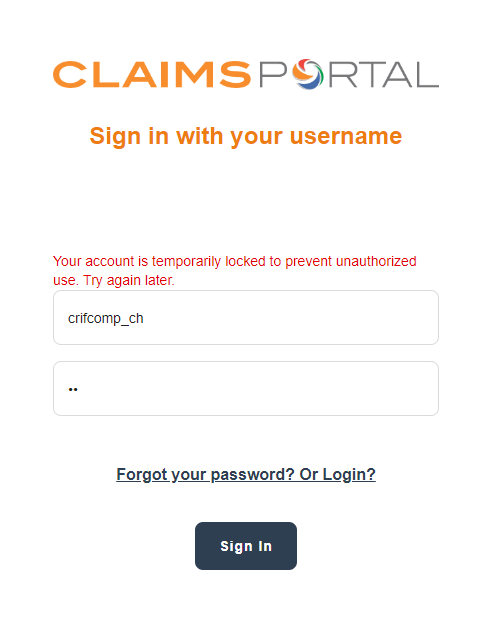
“Your password is incorrect” should be self-explanatory:



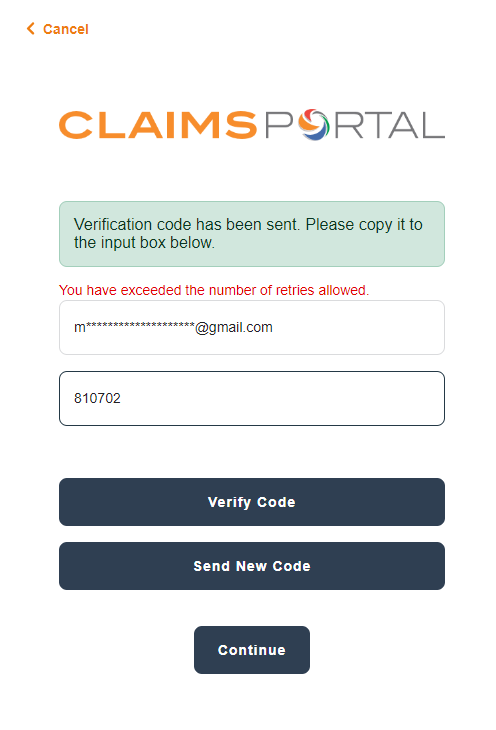
“You have entered the wrong code”, means the OTP is not correct.



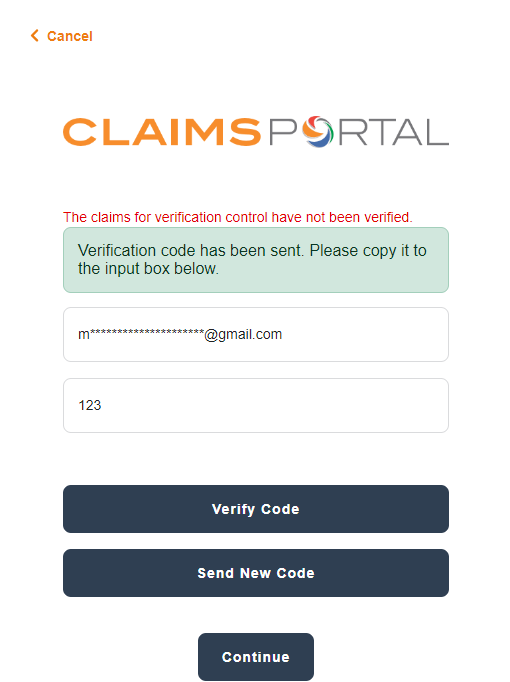
The following message is when the user exceeds the maximum attempts at entering a valid password. Your account is temporarily locked to prevent unauthorised use. Try again later.



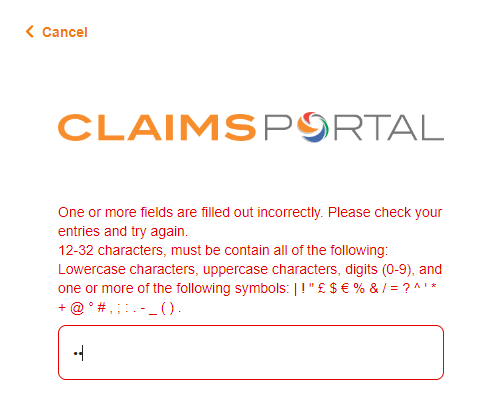
“You have exceeded the numbers of retries allowed”, means the user has exceeded the numbers of attempts to login to the portal:



“The claims for verification control have not been verified” means the user is pressing the “Continue” button without verifying the code first. The user must first verify the OTP and then press “Continue”:



The following error is shown when trying to set a password that does not meet the password validation rules:



The error message "There are too many requests at this moment. Please wait for some time and try again” is when there are too many requests (too many users trying to log in) at the same time or too many users trying to get a token at the same time.

“Your account has been locked. Contact your support person to unlock it, try again.” The account has been disabled via the administrative console (note this is different from the temporary blockage when entering an invalid password).

