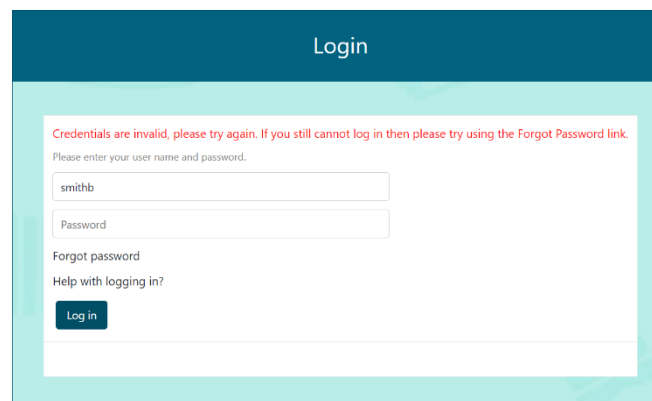# *Troubleshooting* - Ciphr HR login

There are a number of reasons that a user may not be able to login to Ciphr HR. This guide details the most common issues and suggested resolutions.

Credentials are invalid, please try again

- This is generally caused by either the **Username** or the **Password** being incorrectly entered, or the account has been locked
- The user can retry but it is recommended that the user clicks the **Forgot Password** option
- This will prompt the user for their **Username, Email Address, Surname** and **Date of Birth** as validation prior to enabling their password to be reset
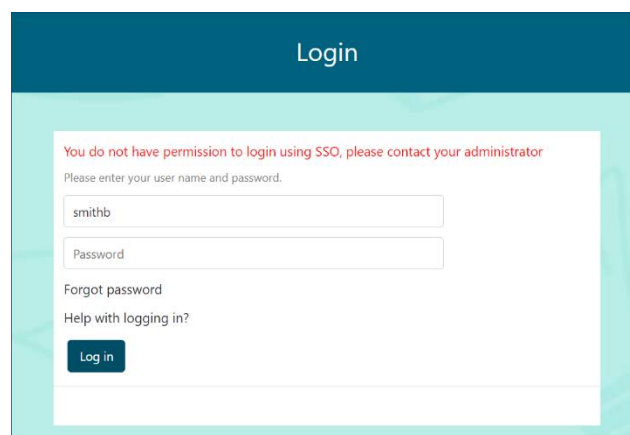

Note: Validation rules for password formats can be created in **System Configuration** as required.

Unable to login with SSO

- When using Ciphr HR with Single Sign On (SSO) the work email address which is stored in Ciphr HR needs to match with the record stored in Active Directory (AD)
- Check AD to ensure that this is the case

Could not find a match……..

- One of the field entries in the screen (right) does not match the data for the user that is recorded in Ciphr HR
- The user will need to contact their System Administrator/HR team to verify that they are entering the correct information

Unexpected Error Message

- As the message would indicate – something has gone wrong which is unexpected
- In order to resolve this the Ciphr HR System Administrator will need to access the user record and go into the **Account Settings** for the user
- Once there click on the options to **Forget Password**, **Forget Secret Answers** and if two factor authentication is being used **Forget TFA Setup**
- The user should then click the **Forgot Password** option on the login screen and then enter the details as required

Verification Code not recognised

- Applicable to customers who are using **Two Factor Authentication** this error indicates that the code has timed out

- It is possible to increase the time limit on a code which is achieved through **System > System Configuration > System Configuration**

- Filter or page through the configuration options and locate the line for **Two Factor Past Windows**

System Configuration

Group Name	Name	Description	Value
Two Factor Auth	External User Two Factor Future Windows	How many codes from windows in the future will be accepted	0
Two Factor Auth	External User Two Factor Past Windows	How many codes from windows in the past will be accepted	1

- The **Value 1** equals 30 seconds
- Click into the **Value,** set as required and then click **Update**

System Configuration

External User Two Factor Past Windows - How many codes from windows in the past will be accepted

Value	1
Default Value	1

✓ Update

Note: Where possible the use of a mobile authentication app is recommended for security reasons.