1. DPS Security Changes

1.1 Introduction

The current DPS account policies do not provide the necessary functionalities for advanced security policies like Two-factor authentication (2FA) to be applied, where a secure token (a 5-digit code) can be sent to user (via email or SMS). This is very similar to what most banks and online stores these days apply, where a verification code is sent to users that needs to be re-entered on the webpage.

With this said we will embark on a journey whereby stricter password policies will be enforced and apply the required changes to the system so we can collect and verify contact details. This allows the system to expose advanced account self-service functionality, whereby users can recover or reset their own passwords, provided that they have verified their cell or email address.

Going forward, on login a 5-digit 2FA verification code will sent to the user via his preferred communication method, which needs to be supplied before access will be granted to the system. 2FA codes will be valid for 12 hours.

Contents

1. DPS Security Changes 1
   1.1 Introduction 1
   1.2 Password Complexity 1
   1.3 Password Expiration 2
   1.4 Password History 2
   1.5 Contact detail verification 3
   1.6 Self Service account management functionality 4
      1.6.1 Self Service password Reset 5
      1.6.2 Self-service account Recovery 8
   1.7 Two Factor Authentication (2FA) 9
      1.7.1 First Login 9
      1.7.2 Resending 2FA codes 11
      1.7.3 Confirm the verification code 11
      1.7.4 Subsequent logins 11

1.2 Password Complexity

All user account password, must meet the following requirements:

1. Password must be at least 12 characters long
2. Password must contain at least one lowercase character
3. Password must contain at least one Uppercase character
4. Password must contain one special character (`, !, #, $, %, ^, &, *, -, _, =, +, ?, ~, |)
5. Password must contain at least one number
6. Password may not contain the following bad password sequences: P@ssw0rd, S3cur1ty, 1qaz@WS

Should a user log into the DPS websites and their password do not meet the above complexity requirements, the user will be redirected to the Reset password page whereby they will be required to update their password to meet the above criteria.

1.3 Password Expiration

User account passwords will expire once every 30 days going forward. If the user's password has expired, they will be redirected to the reset password page and will then be required to create a new password.

1.4 Password History

The DPS system will keep track of previously used passwords and the user will be required create a new password that he hasn't been used before.

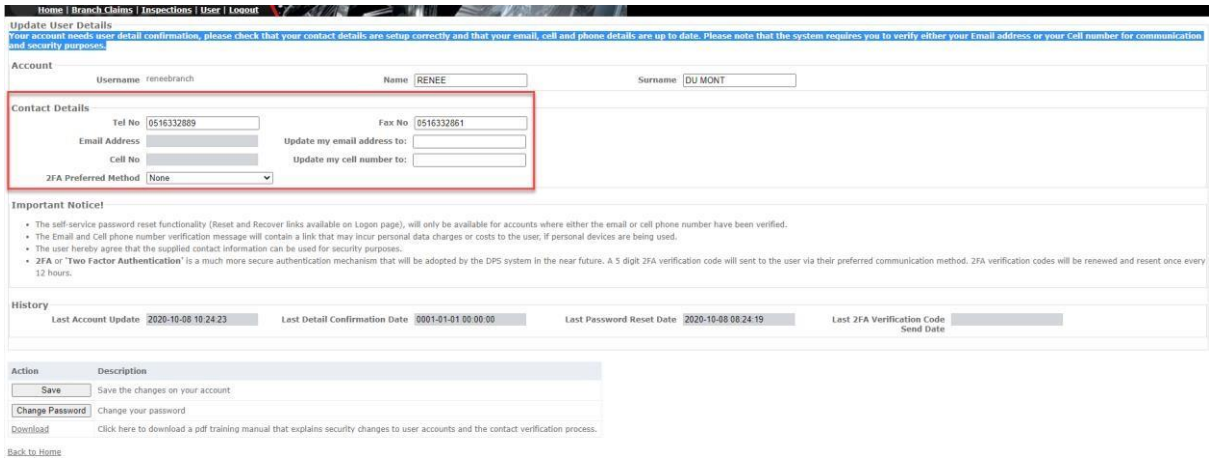
1.5 Contact detail verification

On login, users will be redirected to the account Edit page, until they verify either a cell phone number or an email address.

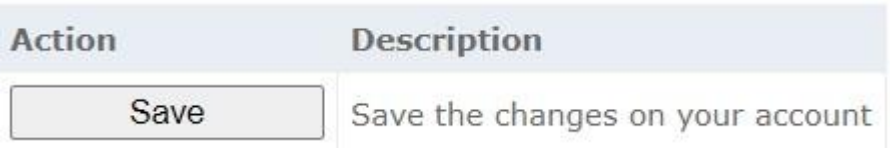
Your account needs user detail confirmation; please check that your contact details are setup correctly and that your email, cell and phone details are up to date. Please note that the system requires you to verify either your Email address or your Cell number for communication and security purposes.

Step 1: Update email address

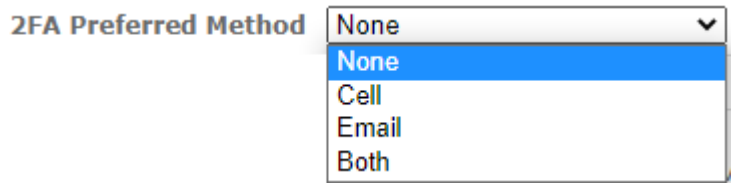
Step 2: Update Cell number



Step 3: Save



Step 4: NB* Please do make use of the 2FA Preferred Method at this point, it will default to none



Step 5:

The user will receive a 5-digit verification code message via an email or SMS.

Enter the verification code / codes received

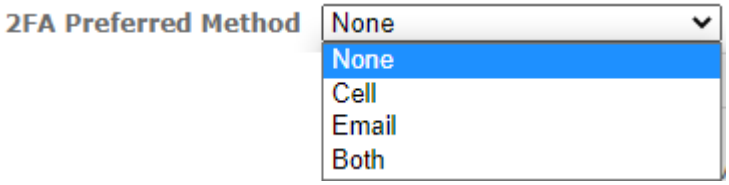


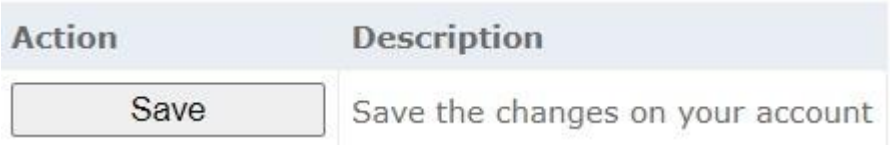
The user must save the changes after entering the verification codes. If the codes are correct, the account will be updated, and the cell phone number and / or email address will be marked as "Verified".



Step 6:

You may now select your 2FA Preferred Method



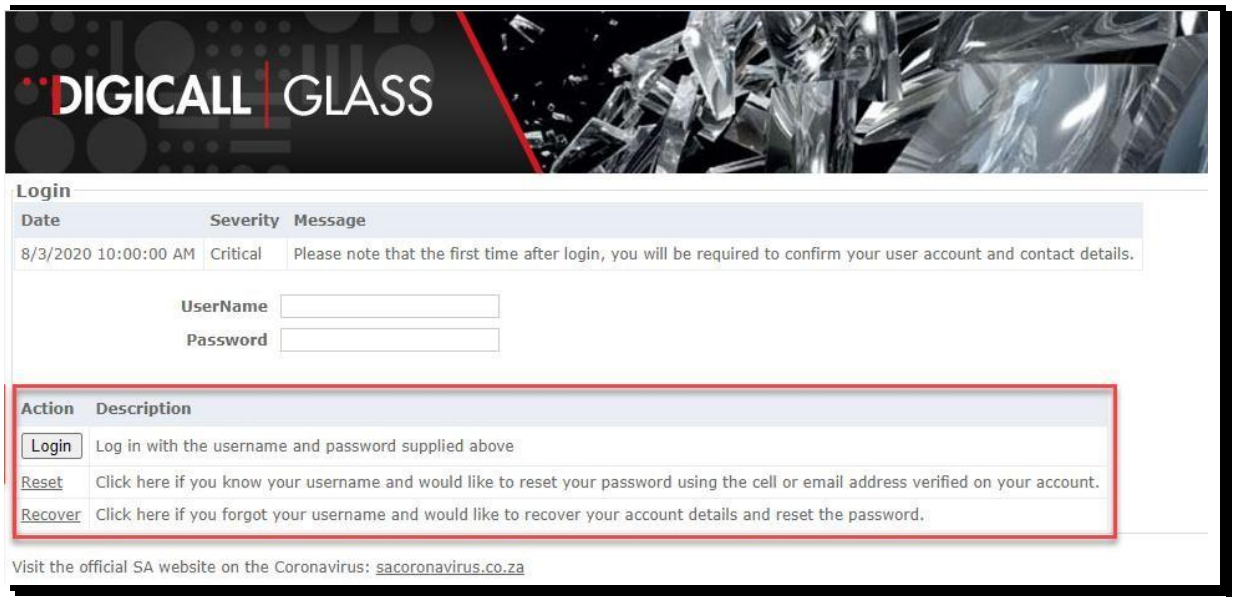


1.6 Self Service account management functionality

There are now 2 additional options that the users can make use of on the logon page of the DPS web portals:

1. **Reset password** - Click here if you know your username and would like to reset your password using the cell or email address verified on your account.

2. Recover: Click here if you forgot your username and would like to recover your account details and reset the password.



1.6.1 Self Service password Reset

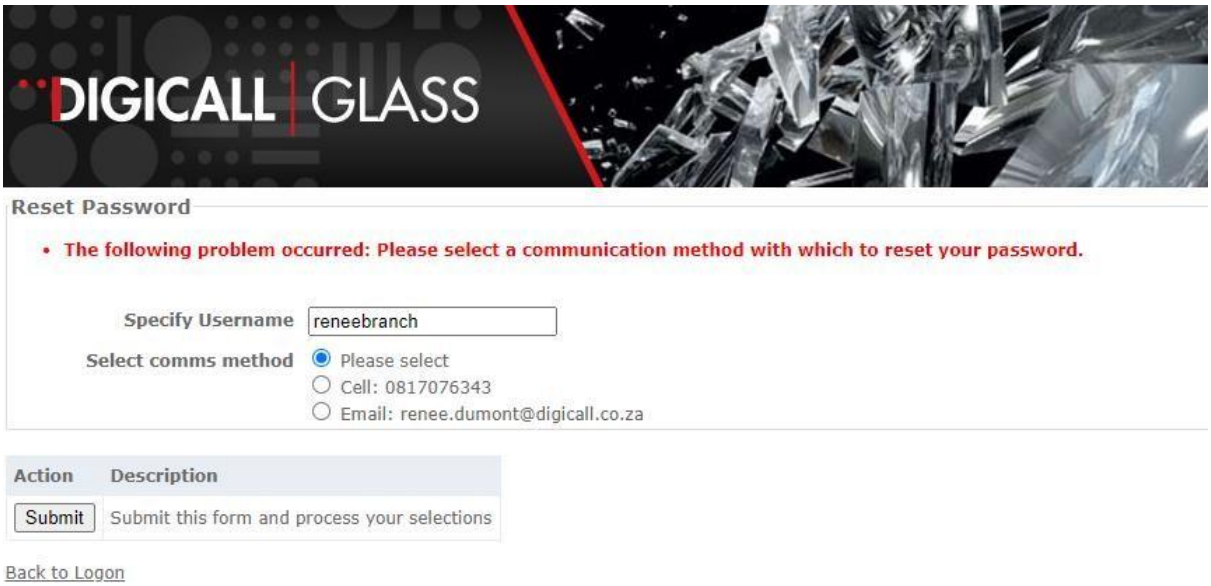
If the user knows their username and would like to perform a password reset on their account, they can make use of the Reset link available on the logon page.

They need to specify their username and complete a “Captcha” to prove to the system that we are dealing with an actual human and not a computer or hacker:



The following message with be displayed:

Please select a communication method with which to reset your password.

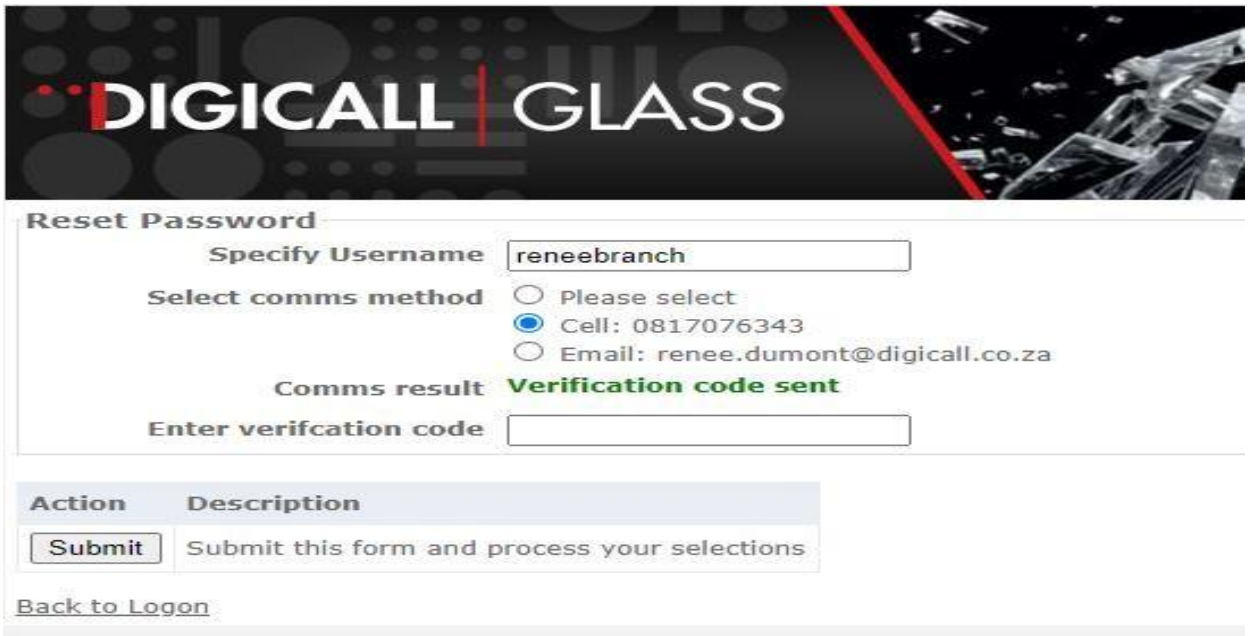


There are two options available when resetting a password either via cell or email.

Note that a password reset will only be available for accounts where the cell and / or email has been verified. (see *1.5 Contact detail verification*)

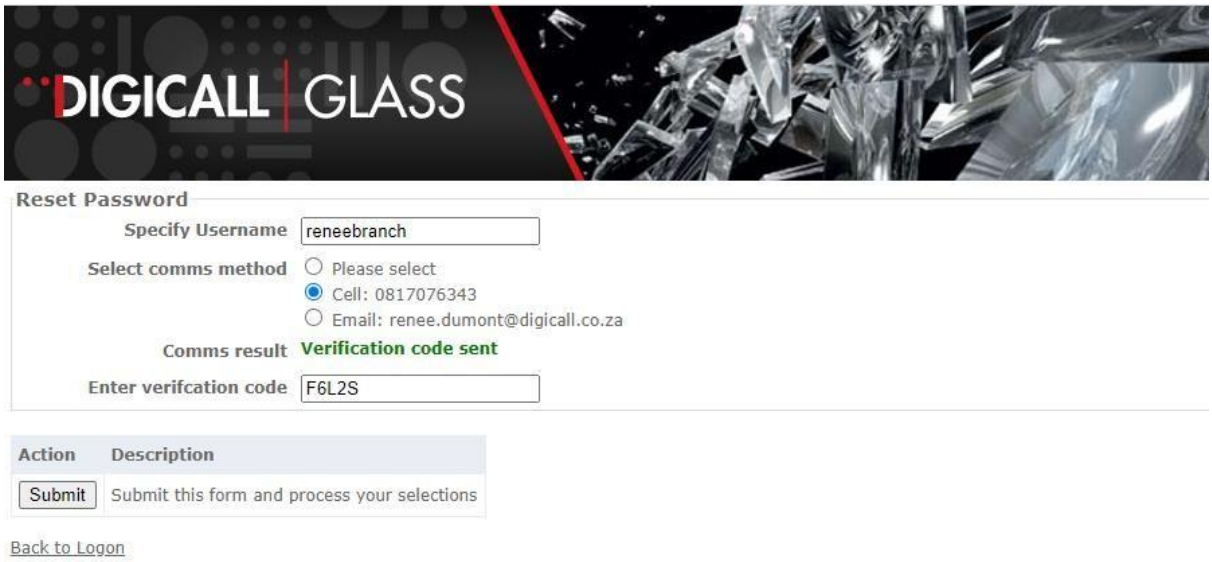
Once you have selected the preferred communication method and click submit, the user will receive the requested communication and on DPS status will state**:**

*"Comms result - **Verification code sent**"*

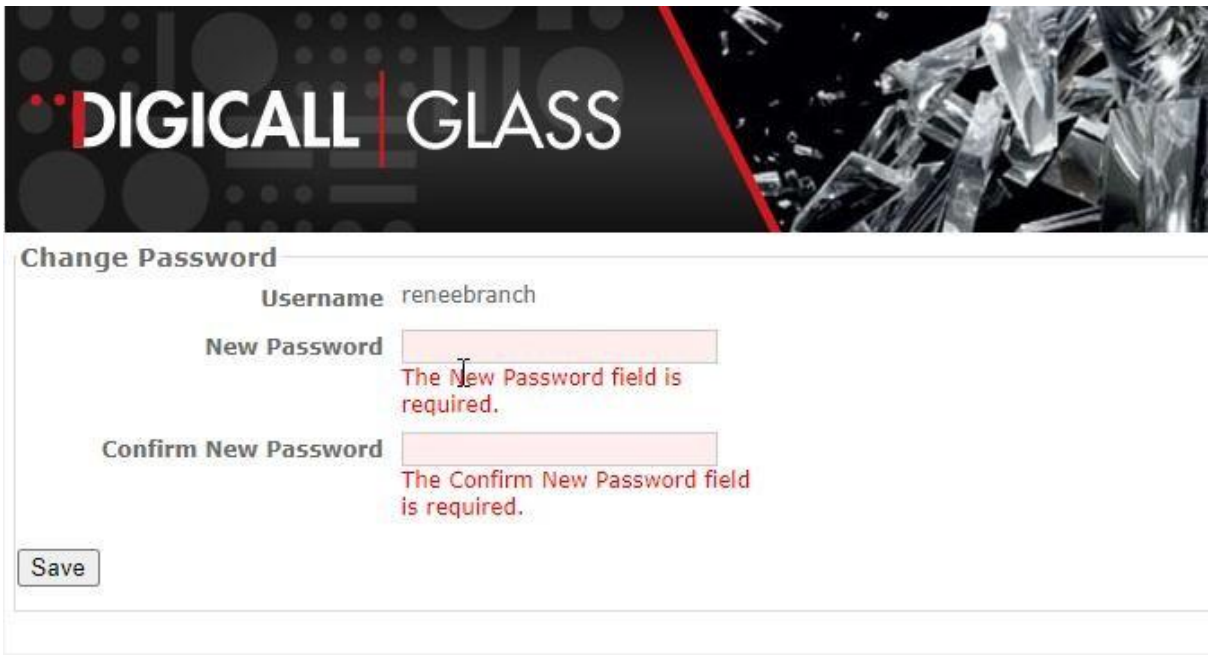


The user will then be required to enter the 5 digit alphanumeric verification code that was sent to their cell phone or email address.

Once done the user will click Submit

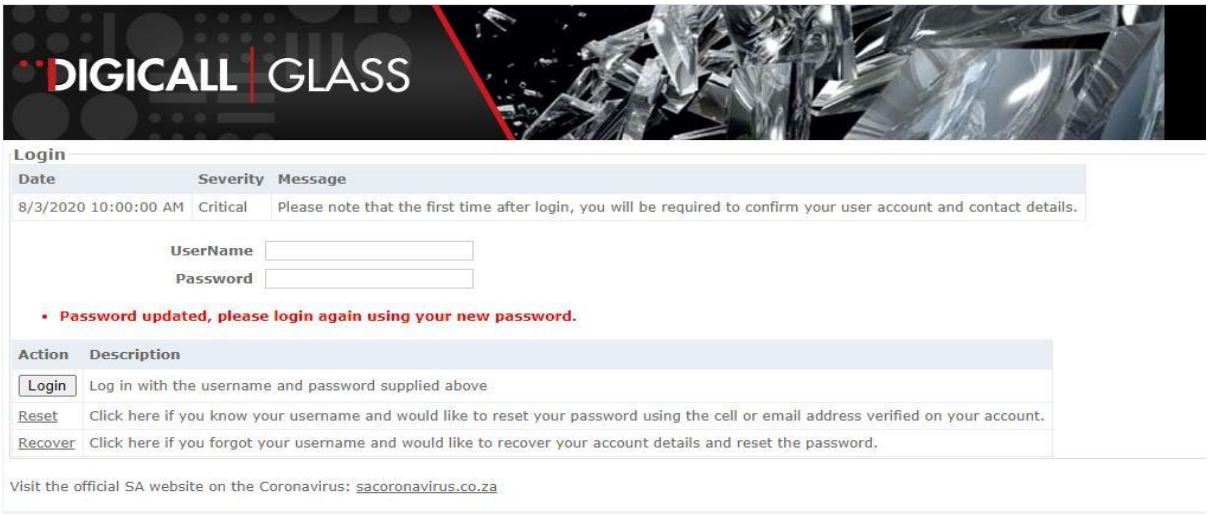


The user will then be presented with a screen which allows the user to change their password.



Once the user has entered and confirmed the new password the user will be redirected back to the main logon page.

Password updated, please login again using your new password

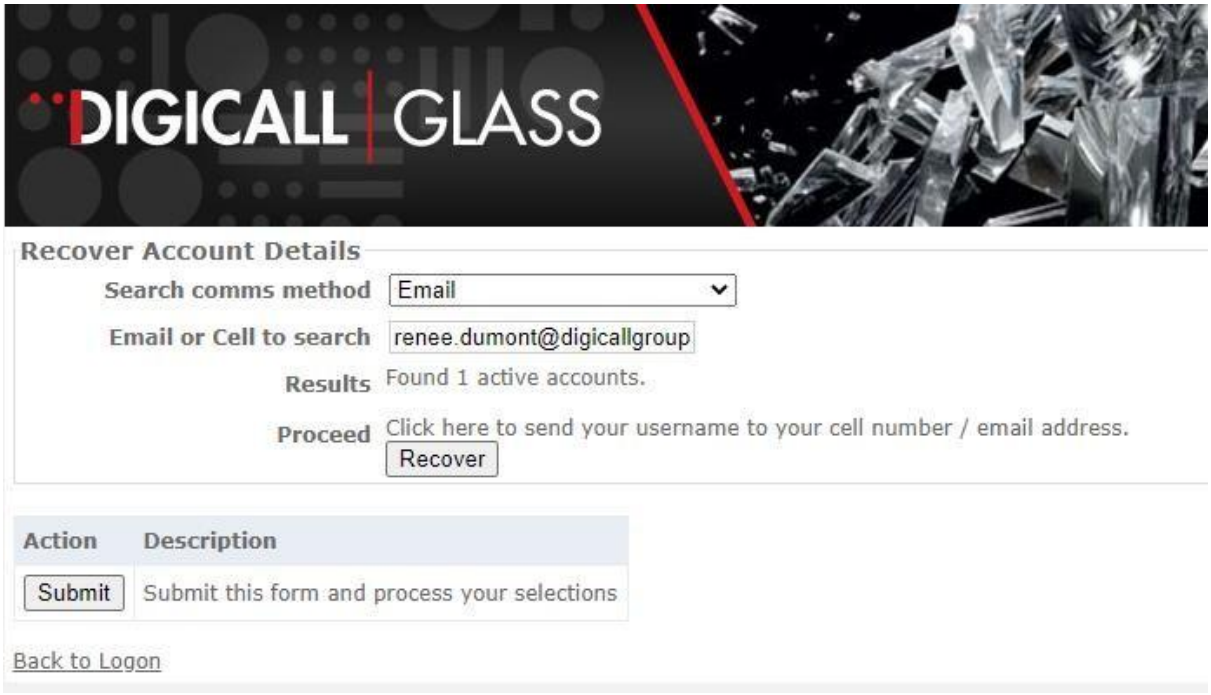


1.6.2 Self-service account Recovery

If the user does not know his username, he may use the “Recover” functionality available on the logon page. The user will be presented with an option to search for his account details, either via their email address or cell phone number, and will be required to complete a Captcha.



Once the preferred selection has been made the user will click on the Recover button:



An email or SMS will be sent to the user that displays the usernames for any active accounts in the DPS system, that use the specified email address or cell phone number.

The user will then be redirected to the standard password reset page (see *1.6.1 Self Service password Reset*), where he can enter the username that was sent to him, so that he can perform a password reset.

1.7 Two Factor Authentication (2FA)

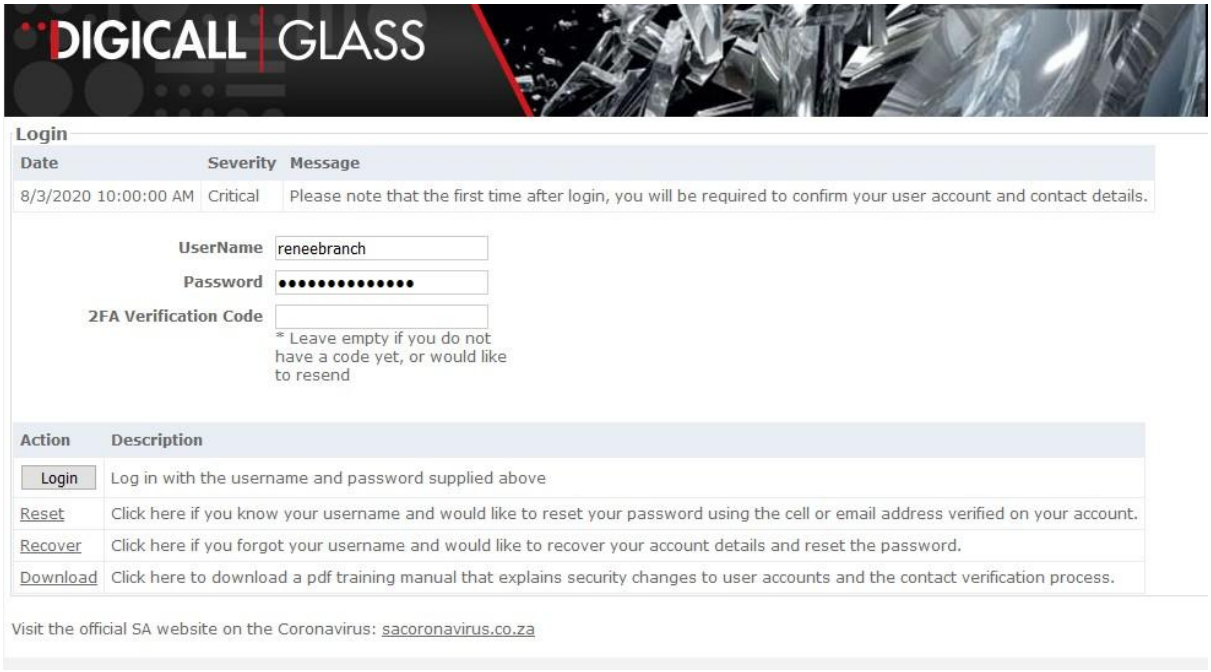
2FA or 'Two Factor Authentication' is a much more secure authentication mechanism that has been incorporated into the System.

On login, a 5-digit 2FA verification code will sent to the user via his preferred communication method, which needs to be supplied before access will be granted to the system. 2FA verification codes will be valid for 12 hours.

If the user account does not have a preferred communication method selected. The user will be able to login without a 2FA code, but his navigation will be restricted to only allow the verification process to be completed. (see *1.5 Contact detail verification*)

1.7.1 First Login

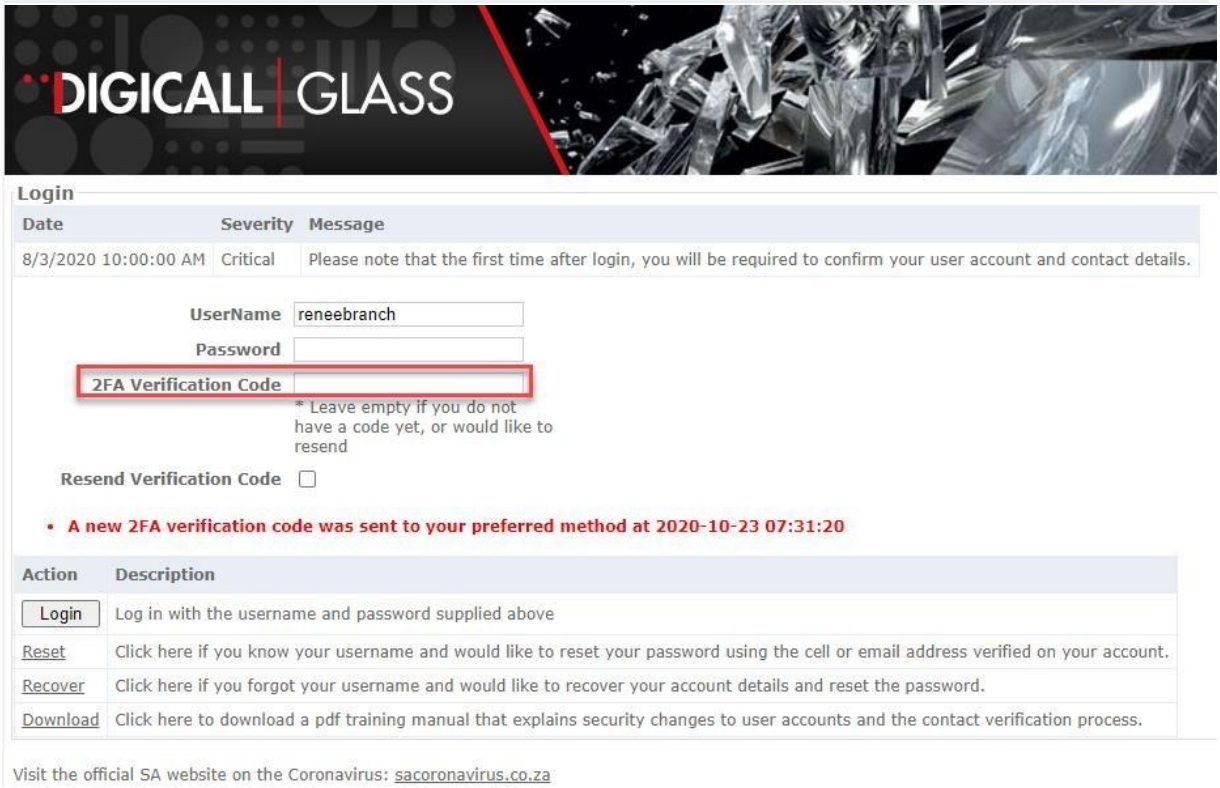
Enter your username and password as per normal but leave the 2FA code blank:



The system will detect if the previous 2FA code is more than 12 hours old (or if none were sent before), in which case it will send a new code to the user via his preferred communication method.

A message will be displayed to the user informing him that a new verification was sent:

- **The 2FA verification code provided do not match the current valid verification code sent at: 2020-10-23 07:31:20**



Note you will now also have the option to “Resend Verification Code” if it was not received.

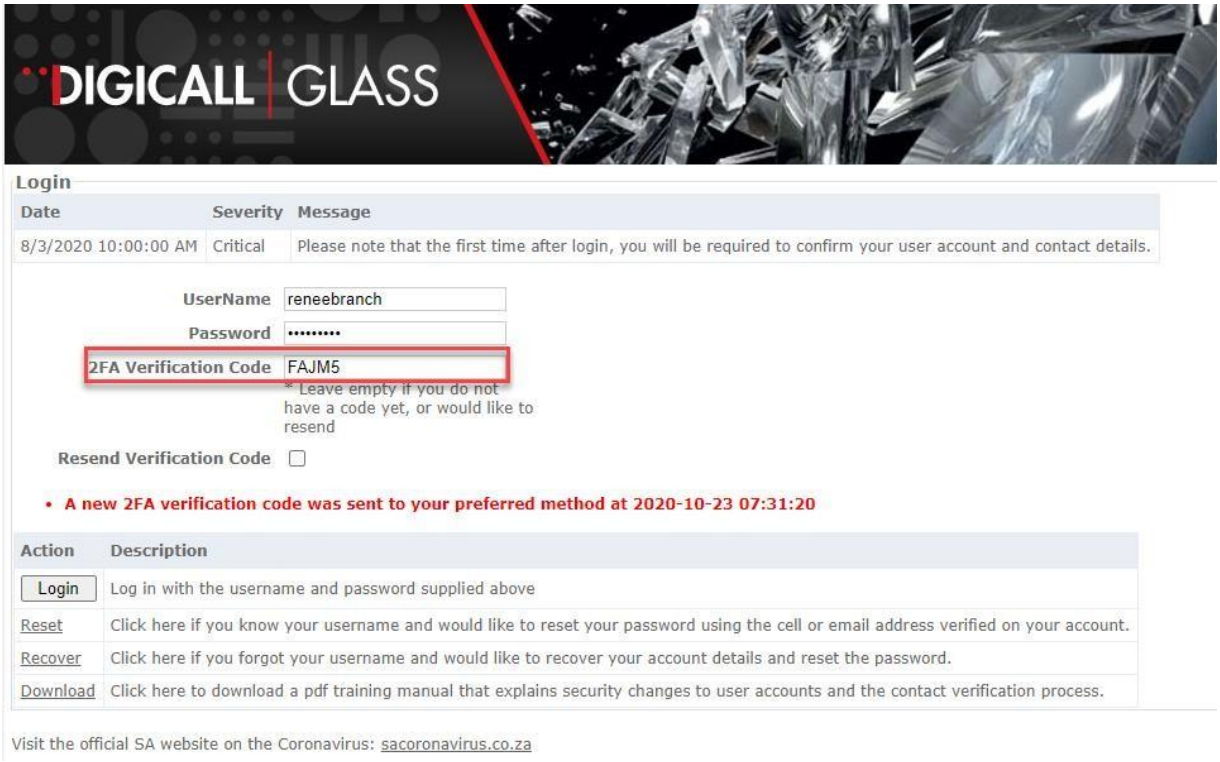
1.7.2 Resending 2FA codes

To resend 2FA codes, login with your username and password and leave the 2FA code blank. The page will refresh and show the "Resend Verification Code" checkbox. Select the checkbox and Login again, then a message will show that the verification code was resent. Please allow some time for communication messages to be delivered via your preferred method.

Depending on network speeds, email service providers and how regularly your email is retrieved or refreshed – it may take some time for 2FA emails to be received. 2FA SMS's should be received within 30 seconds.

1.7.3 Confirm the verification code

Please enter the verification code you received via your preferred comms method in the "2FA Verification Code" textbox:



If the code you entered is valid, the system will log you in.

1.7.4 Subsequent logins

The webpage will remember the previously used 2FA code for 12 hours, so that he does not need to populate this every time he logs in. After 12 hours, the code will expire and the textbox will be blank again.