Login

#### Preconditions:

* Go to page: <https://s.gsb.co.zm/authentication/login>

#### L1: Default country code

* Verify that the default value is “+260”

#### L2: Available country codes

* Verify the list of available values as per [requirements]

***Note****: in the following test cases a decision table is used for the test design:*

| *Username* | *Password* | *Valid* | *Result* |
| --- | --- | --- | --- |
| *Valid* | *Valid* | *Y* | *No errors* |
| *Invalid* | *Valid* | *N* | *Error* |
| *Valid* | *Invalid* | *N* | *Error* |
| *Invalid* | *Invalid* | *N* | *Error* |

#### L3: Phone number input

* “Phone” changes to “Phone number” label on focus
* “Phone number is required” validation on lost focus and empty input
* “Mobile provider prefix is not correct” validation [bug]
* “Incorrect phone number” validation [missing due to the bug]
* Valid phone number: no validation errors on lost focus

*Valid phone numbers as per [requirements], e.g.*

*Correct Length (8 digits) 01234567*

*Correct Length + 1 - should be trimmed to 8 digits*

*Invalid phone numbers as per [requirements], e.g.*

***Boundary Values***

*Too short (1,7 digits) 0, 1234567*

*Too long (9 digits) - will be trimmed to 8 digits*

#### L4: Password input

* “ Show/hide password” icon
* “Password is required” validation on lost focus and empty input
* Login as user with valid passwords:

*Valid passwords as per [requirements], e.g.*

***Boundary Values***

*Minimum Length (7 chars) abc1234 Minimum Length + 1 (8 chars) test2025*

*Typical Mid-Length (10 chars) P@ssword10*

*Just Below Maximum Length (19 chars) ThisIsAValidPass19*

*Maximum Length (20 chars) Max20CharsPass#2025!*

*Special Character at Start #TestPass12*

*Special Character at End Pass12Test!*

*Only Numbers (if allowed) 12345678*

*Only Letters (if allowed) abcdefgh*

*Mixed Case Sensitivity CaseTest12*

*Repeated Characters aaaaaaa1*

*Please use a data provider for automation.*

* Login as user with invalid password and valid phone number:

*Invalid passwords as per [requirements], e.g.*

***Boundary Values***

*Too Short (6 chars, assuming min is 7) abc123*

*Too Short (Empty password) ``*

*Too Long (21 chars, assuming max is 20) ThisPasswordIsTooLong123!*

*Only Spaces*

*Only Numbers (if letters are required) 12345678*

*Only Letters (if numbers are required) abcdefgh*

*No Uppercase (if required) password123!*

*No Lowercase (if required) PASSWORD123!*

*No Special Characters (if required) Password123*

*Leading Space password1*

*Trailing Space password1*

*Repeated Characters Only aaaaaaaa*

*Common Weak Password password1*

*Please use a data provider for automation.*

#### L5: Forgot Password? link

* Clicking on “Forgot Password?” redirects to: <https://s.gsb.co.zm/authentication/forgot> in the same tab

#### L6: Login button

* Click on login with empty fields: same validation as on lost focus
* Click on login with incorrect credentials: same validation as on lost focus
* Login with valid credentials: use multiple users with various combinations of valid phone/password - [https://s.gsb.co.zm/authentication/](https://s.gsb.co.zm/authentication/forgot)[dashboard] page is opened. User is logged in.

#### L7: “REGISTER” link

* Clicking on “REGISTER” redirects to: <https://s.gsb.co.zm/authentication/register> in the same tab

**Final Notes:**

To finalize the test cases for the automation a mix of multiple design techniques is required:

1. Decision tables for combinations of expected results
2. Boundary values for setting up users with correct/incorrect credentials
3. State transition diagrams to combine the scenarios into more complex flows (E2E cases to test other functions)
4. Pairwise design to reduce the number of tests (especially on invalid credentials pairs)

The templates for the test cases should be decided with the team. I personally chose to KISS as possible.