# E2E Test Plan of **Logins Management Page**

For

OneLocal

*Created by:*

Farhana Rahman

January 28, 2024

Version:1.0

## Index

**Introduction:**

This test plan is designed to:

- Describe approach used by me during testing.
- Organize and implement the testing process.
- Define the test deliverables.

**Scope:**

As per requirement, initial scope is end-to-end testing of Logins Management page of OneLocal mainly focusing onto the Logins module where the users get requests to submit credentials for their Website/Instagram/CRM etc. as well as Other Accounts module such as Mindbody where users can connect third-party integrations for automated workflows.

**Objective:**

The objective of this assessment is to assess the overall performance of the Logins Management page of OneLocal's web application from a grey-box perspective. This includes test cases for the Logins Management webpage that are crucial to ensure system security and user experience. Overall, these test cases are vital to uncovering potential vulnerabilities, guaranteeing a robust credentials update, and integrating third-party applications mechanism. Some of these test cases will be used in automation testing in a robust automation framework.

**Methodology:**

I will explore the Logins Management page of the application to look for all the potential test cases that can be used for testing. I will perform manual end-to-end testing to check for problems not typically found by tools. Based on the manual testing and the test cases available I will perform Selenium Automation testing on 3 test scenarios to automate my testing.

**Environment Requirements:**

Windows 11, version 22H2, HP PC- 16GB RAM intel core i7 processor, Chrome browser/Firefox, IntelliJ IDE, Java IDK, Apache Maven, Selenium WebDriver, TestNG, Cucumber BDD framework, GitHub

**Test Scenarios and Test Cases:**

The following test scenarios and test cases are crucial to ensure functionality, system security and user experience of Logins Management Page.

***Functional Test Scenarios of Logins Management page***

| Module | Test Cases |
|---|---|
| **Required Logins** | Verify a second window/form displays for Update Credentials when user clicks on the Update button |
| | Verify the cursor is focused on the input field of Username and Password when clicked on the fields |
| | Verify minimum and maximum lengths is set for all input fields |
| | Verify user can successfully Submit Credentials after changing username and password within specified length limits |
| | Verify user cannot successfully Submit Credentials after changing password with special characters only |
| | Verify Update Credentials form closes when user clicks Dismiss button |
| | Verify validation message is displayed in case when user leaves Username and/or password fields blank |
| | Verify validation message is displayed in case of exceeding the character limit of the Username and password fields |
| | Verify Password field accepts only 8 characters, numbers, and special symbols |
| | Verify successful login to Required Logins (Website, Instagram, CRM etc.) after updating credentials |
| | Verify unsuccessful login to Required Logins (Website, Instagram, CRM etc.) with invalid credentials after updating on Login Management page |
| | Verify clicking browser back button at any step of updating credentials take the user to the Logins Management page |
| **Other Accounts** | Verify user can navigate to appropriate Sign In page of Google Analytics/Stripe/Acuity/QuickBooks when the respective Account's Connect button is clicked |
| | Verify a second window/form titled Enter Site ID opens when user clicks Connect buttons of Jane/Mindbody Account |
| | Verify user views error message with launch instructions when Connect button of Square Account is clicked |
| | Verify Enter Site ID Credentials form closes when user clicks Dismiss button |
| | Verify validation message is displayed when user leaves Enter Site ID field blank |
| | Verify user can view Activation instructions after entering Enter Site ID |
| | Verify user can Sign-In to Accounts of Jane / Mindbody after successful activation |
| | Verify user is directed to the appropriate page when clicking on links on Enter Site ID form |
| | Verify user goes back to Enter Site ID page when Back button is clicked on Activation page |
| | Verify user is directed to Enter Site ID/Activation pages when Next button is clicked |
| | Verify clicking browser back button at any step in Enter Site ID takes the user to the Logins Management page |

### *Non-functional Security Test Cases of Logins Management Page*

| Test Cases |
|---|
| Verify the presence of HTTPS to ensure secure data transmission |
| Verify a validation message after a specified number of credentials update |
| Verify monitoring user account activity for detecting suspicious behavior |
| Verify session timeout functionality for automatic logout after inactivity. |
| Verify clicking on the browser back button after successful sign out should not take user to a logged-in mode |

### *UI Test Scenarios of Logins Management Page*

| Test Scenarios | Test Cases |
|---|---|
| *Verify the visibility of elements:* | Confirm the visibility of Required Logins (Website Logins, Instagram, CRM Logins etc.) and Other Accounts (Google Analytics, Stripe, Mindbody etc.) |
| | Ensure the visibility and clarity of the Update button for each of the Required Logins and Connect button for each of the Other Accounts |
| | Verify accessibility of the Update and Connect buttons |
| | Confirm visibility of Update Credentials form |
| | Check visibility of static instruction message at the top including username and password reset instructions |
| | Check visibility of URL, Username and Password elements |
| | Confirm the visibility of URL address and that the auto-populated URL represents respective login type and that it cannot be changed by user |
| | Check the visibility of Username and Password input fields and have auto-populated credentials |
| | Check the lines for input fields of Username and Password turns blue when clicked on the fields |
| | Check if password is displayed in masked format rather than actual text format. |
| | Ensure the visibility of two buttons – Dismiss and Submit Credentials |
| | Check availability and visibility of Clear/Reset button to clear all data in input fields |
| | Verify accessibility of Dismiss button |
| | Confirm that Submit Credentials button is initially disabled |
| | Confirm that Submit Credentials button is enabled once Username and/or Password is changed |
| | Verify to see if the font style and size of the labels, as well as the text on each object are clearly visible |
| *Verify field validations:* | Check if the Username and Password input fields are present on the Update Credentials page and have auto-populated valid credentials |

| | |
|---|---|
| | Check if the credentials update is successful after changing the Username/Password |
| | Test the system’s behavior when entering more characters than the allowed limit for both Username and Password |
| | Validate that the system restricts submit attempts after reaching a defined limit for both Username and Password and displays an appropriate message |
| *Verify error messages:* | Input fields should display appropriate validation messages when any or both Username and Password are empty |
| | Ensure the system validates and displays an error for an invalid username format (e.g. special characters) |
| | Validate the system’s response to an invalid password format, triggering an error message |
| *Verify working buttons:* | Validate that clicking the Update button displays a small form of Update Credentials |
| | Check that clicking Dismiss button enables the user to view the Login Management page and small form of Update Credentials auto-closes |
| | Verify that clicking enabled Submit Credentials button successfully submits the valid changed credentials and auto-closes Update Credentials form |
| | Verify that disabled Submit Credentials button will not be clickable until the credentials are changed |
| | Validate that clicking the Connect button directs users to the respective Account’s Sign In page or a second form for entering site ID, activation and then sign in |
| *Verify responsiveness and compatibility* | Test the Login Management page’s responsiveness on different screen sizes, including desktop, tablet and mobile |
| | Ensure consistent visibility and functionality across various web browsers |
| | Confirm text and font sizes adjust appropriately for different screen sizes |
| | Check that buttons and elements maintain proper placement and spacing on different devices |

**Responsibilities / Effort Required:**

- Manual E2E testing.
- Automation framework: Installation of IntelliJ, downloading Java JDK, creating Apache Maven project, adding dependencies to pom.xml file, creating packages, folders, feature files and java classes for test scenarios in Gherkin language, for test scripts in step definitions folder, runner class for executing automation tests using TestNG.
- From the above test cases, the following are to be used for automation:

- Verify user can successfully Submit Credentials after changing username and password within specified length limits.
- Verify that validation message is displayed in case when user leaves Username and/or password fields blank.
- Verify user is directed to the appropriate page when clicking on links on Enter Site ID form.

**Risks, Constraints, Assumptions, Dependencies:**

- Versions of browsers vary from device to device, non-availability of latest version of chrome driver.
- Limitations to access to third party integrations thus limiting exploring the application.
- Input fields reset or update instructions are not available, thus limiting target test cases.
- Updated versions of dependencies can be used by changing the version in the pom.xml file.
- In case of a different testing environment or change in web elements, automated test scripts must be updated.