

Name: ENG \ Kerolos George Attia

Leader ENG \ Abdelrahman Ramadan

1-Authentication Module (AUTH)

Login Requirements:

AUTH-001: Username field cannot be blank and must accept only registered usernames.

AUTH-002: Password field cannot be blank and must accept only valid passwords.

AUTH-003: Successful login must redirect to Account Overview page.

AUTH-004: Invalid credentials must display error: "The username and password could not be verified."

AUTH-005: Blank username or password must display error: "Please enter a username and password."

Password Recovery Requirements:

AUTH-006: Clicking "Forgot Login Info" must open lookup functionality.

AUTH-007: All fields in password recovery are mandatory.

AUTH-008: Valid registered data must display account information.

AUTH-009: Invalid data must display error: "The customer information provided could not be found."

AUTH-010: Support session persistence during navigation until logout.

2-Objective

The objective of testing the Authentication module is to ensure that all login and password recovery functionalities operate securely, accurately, and according to business requirements. This includes validating correct handling of registered and unregistered credentials, verifying system responses to blank or invalid inputs, ensuring

secure session management, and confirming that password reset flows generate a valid temporary password within the required timeframe. The goal is to validate functional correctness, error handling, usability flows, and compliance with authentication standards.

3- Scope

In-Scope

- Validation of login functionality (successful and unsuccessful attempts).
- Verification of username and password field validations.
- Error messages for invalid or blank credentials.
- Redirect behavior after successful login.
- "Forgot Login Info" workflow.
- Mandatory field validation in password recovery.
- Validation of lookup functionality for registered and unregistered customers.
- Verification of correct display of account information for valid recovery data.
- Error handling for invalid recovery data.
- Temporary password generation via email/SMS.
- Session persistence until logout.

Out-of-Scope

- UI styling and layout testing.
- Performance, load, and stress testing.
- External email/SMS system performance (only functional check is included).
- Penetration testing and advanced security testing.

4- Test Approach

- Manual functional testing will be performed for all login and password recovery requirements.
- Each requirement (AUTH-001 to AUTH-011) will be validated individually with positive and negative test scenarios.
- Field-level validation will be tested for blank entries, invalid formats, and valid registered credentials.
- Error messages will be checked for accuracy, correctness, and alignment with requirements.
- Redirection behavior will be validated after successful login.
- Password recovery flow will be tested using valid and invalid user information.
- Verification email/SMS functionality will be checked by validating the temporary password is generated and usable.
- Session management tests will verify that user sessions persist during normal navigation and end properly after logout.
- Test results will be documented, and defects will be reported with request/response logs and screenshots.

5- Test Techniques

- **Equivalence Partitioning (EP):**
Categorizing inputs into valid and invalid partitions for username, password, and recovery fields.
- **Boundary Value Analysis (BVA):**
Applying limits on username/password length (min/max characters if applicable).
- **Positive & Negative Testing:**
Validating correct login with valid inputs and proper rejection of invalid ones.

- **Error Guessing:**
Predicting common issues such as spaces-only input, expired temporary passwords, incorrect capitalization.
 - **Use Case Testing:**
Validating real-world flows such as "Login → Navigate → Logout".
 - **State Transition Testing:**
Ensuring session states change correctly (Logged Out → Logged In → Logged Out).
-