

Test Cases and Hypothetical Test Reports

Role-Based Internal Platform for Targeted Content Delivery

Version 1.0.0

Group 20
Jesus Calvo,
Justin Gip
Shane Guzman
Samuel Mekonnen

December 5, 2025
CS 3338-01 (94305)

Contents

1	Introduction	3
2	Test Strategy Overview	3
2.1	Scope	3
2.2	Test Levels	3
2.3	Test Management	3
3	Snapshot 1 Test Cases: Authentication and Basic Navigation	3
3.1	Scope	3
3.2	Test Cases	4
3.3	Hypothetical Snapshot 1 Test Report	5
4	Snapshot 2 Test Cases: Content Management and Targeting	6
4.1	Scope	6
4.2	Test Cases	6
4.3	Hypothetical Snapshot 2 Test Report	7
5	Snapshot 3 Test Cases: Targeted Feed, Acknowledgements, and Reporting	8
5.1	Scope	8
5.2	Test Cases	8
5.3	Hypothetical Snapshot 3 Test Report	9
6	Snapshot 4 Test Cases: Administration and Regression	10
6.1	Scope	10
6.2	Test Cases	10
6.3	Hypothetical Snapshot 4 Test Report	11
7	Appendix A: Requirement-to-Test Traceability (Partial)	12

1 Introduction

This document describes the functional test cases and test execution reports for the **Role-Based Internal Platform for Targeted Content Delivery**. Test cases are derived from the Software Requirements Specification (SRS) and Software Design Document (SDD) and grouped by project snapshot.

Each test case includes:

- A unique Test Case ID.
- Related functional requirement(s) (FR-*nn*).
- Preconditions.
- Test steps.
- Expected results.

For each snapshot a short, test report is provided, summarizing the imagined outcome of executing these tests and how they relate to the implemented Jira work items.

2 Test Strategy Overview

2.1 Scope

The test cases in this document focus on validating key behaviors of:

- User authentication and authorization.
- Content management and targeting.
- Targeted content feed and acknowledgements.
- Reporting and administration features.

Nonfunctional requirements (performance, security, usability) are touched by a small number of high-level tests.

2.2 Test Levels

- **Unit tests** for core business logic (e.g., targeting engine, acknowledgement rules).
- **API-level integration tests** for endpoints like `/api/auth/login`, `/api/content`, `/api/feed`, and `/api/events`.
- **UI/system tests** for end-to-end flows executed via the web interface.

2.3 Test Management

In a real deployment, tests would be tracked using:

- Jira issues for each feature and defect.
- A testing section or board within the Jira project for organizing manual and automated test runs.

For the purpose of this course project, this document serves as the primary record of test cases and reports.

3 Snapshot 1 Test Cases: Authentication and Basic Navigation

3.1 Scope

Snapshot 1 focuses on:

- User login and basic RBAC (FR-01–FR-05).
- Minimal dashboard after login.

3.2 Test Cases

TC-1.1: Login with Valid Credentials

- **Related Requirements:** FR-01, FR-02, FR-03
- **Preconditions:**
 - User `employee1@example.com` exists with a known password.
 - User account is active.
- **Steps:**
 1. Navigate to the Login page.
 2. Enter valid email and password for `employee1@example.com`.
 3. Click the **Login** button.
- **Expected Result:**
 - User is redirected to the dashboard page.
 - A valid session or token is created.
 - Protected pages can now be accessed without being redirected back to login.

TC-1.2: Login with Invalid Password

- **Related Requirements:** FR-01, FR-02
- **Preconditions:**
 - User `employee1@example.com` exists.
- **Steps:**
 1. Navigate to the Login page.
 2. Enter correct email but an incorrect password.
 3. Click the **Login** button.
- **Expected Result:**
 - Login attempt is rejected.
 - An error message such as “Invalid email or password” is shown.
 - No session or token is created.

TC-1.3: Access Protected Page When Not Authenticated

- **Related Requirements:** FR-03
- **Preconditions:**
 - No active session or token.
- **Steps:**
 1. Attempt to directly open the dashboard URL in the browser.
- **Expected Result:**
 - User is redirected to the login page OR receives a `401 Unauthorized` response.
 - No dashboard content is displayed.

TC-1.4: Role-Based Access to Admin Console

- **Related Requirements:** FR-04, FR-05
- **Preconditions:**
 - `employee1` has the `Employee` role only.
 - `admin1` has the `Content Administrator` role.
- **Steps:**
 1. Log in as `employee1`. Attempt to open Admin Console.
 2. Log out, then log in as `admin1`. Open Admin Console.
- **Expected Result:**
 - `employee1` is denied access (error message or redirect).
 - `admin1` can access Admin Console successfully.

3.3 Hypothetical Snapshot 1 Test Report

Snapshot 1 Test Execution Summary (Hypothetical)

Test Case Group	# Cases	Passed	Failed	Blocked	
Authentication (TC-1.1–TC-1.3)	3	3	0	0	
Role-Based Access (TC-1.4)	1	1	0	0	
Total	4	4	0	0	

Summary (Hypothetical): All Snapshot 1 tests passed. Basic authentication and RBAC are functioning as expected, providing a stable foundation for later snapshots.

4 Snapshot 2 Test Cases: Content Management and Targeting

4.1 Scope

Snapshot 2 adds content management and initial targeting logic:

- Content creation, scheduling, and archiving (FR-06–FR-10).
- Attribute-based targeting rules (FR-11–FR-14).

4.2 Test Cases

TC-2.1: Create Content Item with Valid Data

- **Related Requirements:** FR-06
- **Preconditions:**
 - Logged in as `Content Administrator`.
- **Steps:**
 1. Navigate to **Create Content** page.
 2. Enter title, body, and select category and tags.
 3. Click **Save**.
- **Expected Result:**
 - New content item is persisted and appears in Admin Content List.
 - No validation errors are displayed.

TC-2.2: Reject Content Creation with Missing Title

- **Related Requirements:** FR-06
- **Preconditions:** Logged in as `Content Administrator`.
- **Steps:**
 1. Open **Create Content**.
 2. Leave title empty; fill in body and category.
 3. Click **Save**.
- **Expected Result:**
 - Content is not saved.
 - Validation error indicates title is required.

TC-2.3: Schedule Content Using Start and End Dates

- **Related Requirements:** FR-07, FR-19
- **Preconditions:**
 - Logged in as `Content Administrator`.
 - Current date is between two known dates.
- **Steps:**
 1. Create content C1 with start date = today and end date = today + 7 days.
 2. Create content C2 with end date = yesterday.
 3. Log in as `employee1` and view feed.
- **Expected Result:**
 - C1 is visible in the feed.
 - C2 is not visible because it has expired.

TC-2.4: Archive Content Item

- **Related Requirements:** FR-10
- **Preconditions:**
 - An active content item C3 exists.
- **Steps:**
 1. As **Content Administrator**, open C3 in the Admin Content List.
 2. Click **Archive** and confirm.
 3. Log in as targeted end user and view feed.
- **Expected Result:**
 - C3 is no longer shown to end users.
 - C3 appears with status **Archived** in Admin Content List.

TC-2.5: Simple Role-Based Targeting Rule

- **Related Requirements:** FR-11, FR-13
- **Preconditions:**
 - User **employee1** with role = Employee.
 - User **manager1** with role = Manager.
- **Steps:**
 1. Create content C4 targeted to role = Manager.
 2. Log in as **employee1** and view feed.
 3. Log in as **manager1** and view feed.
- **Expected Result:**
 - **employee1** does not see C4.
 - **manager1** sees C4 in the feed.

TC-2.6: Update Targeting After Role Change

- **Related Requirements:** FR-14
- **Preconditions:**
 - Content C5 targeted to role = Manager.
 - User **employee2** currently role = Employee.
- **Steps:**
 1. Log in as **employee2**; verify C5 is not visible.
 2. Change **employee2**'s role to Manager using User Administration.
 3. Log in again as **employee2** and view feed.
- **Expected Result:**
 - Initially C5 is not in the feed.
 - After role change, C5 appears for **employee2**.

4.3 Hypothetical Snapshot 2 Test Report

Summary (Hypothetical): One failure occurred in TC-2.3, where expired content still appeared in the feed due to an off-by-one comparison bug on end dates. A Jira bug ticket was created and fixed in Snapshot 3.

Snapshot 2 Test Execution Summary (Hypothetical)

Test Case Group	# Cases	Passed	Failed	Blocked
Content Creation and Validation (TC-2.1–TC-2.2)	2	2	0	0
Scheduling and Archiving (TC-2.3–TC-2.4)	2	1	1	0
Targeting Rules (TC-2.5–TC-2.6)	2	2	0	0
Total	6	5	1	0

5 Snapshot 3 Test Cases: Targeted Feed, Acknowledgements, and Reporting**5.1 Scope**

Snapshot 3 delivers:

- Targeted content feed (FR-15–FR-19).
- View and acknowledgement tracking (FR-20–FR-23).
- Initial reporting (FR-24–FR-26).

5.2 Test Cases**TC-3.1: Personalized Feed Shows Only Targeted Content**

- **Related Requirements:** FR-15, FR-19

- **Preconditions:**

- Content C6 targeted to role = Employee.
- Content C7 targeted to role = Manager.
- User `employee1` has role = Employee.

- **Steps:**

1. Log in as `employee1`.
2. Open End User Dashboard.

- **Expected Result:**

- C6 appears in feed.
- C7 does not appear in feed.

TC-3.2: Feed Filtering by Category

- **Related Requirements:** FR-17

- **Preconditions:**

- Two visible content items exist: C8 (category = Compliance) and C9 (category = General).

- **Steps:**

1. Log in and open dashboard.
2. Apply filter **Category = Compliance**.

- **Expected Result:**

- C8 remains visible.
- C9 is hidden from the list.

TC-3.3: Search Content by Keyword

- **Related Requirements:** FR-18
- **Steps:**
 1. Ensure there is content C10 with the title “Privacy Policy Update”.
 2. Enter keyword “Privacy” into search box.
- **Expected Result:**
 - C10 appears in search results.
 - Unrelated content is excluded from results.

TC-3.4: Record View Event when Content is Opened

- **Related Requirements:** FR-20
- **Steps:**
 1. Log in as `employee1`.
 2. Open detail page for content C11.
 3. Query `DeliveryEvent` table or reporting API for events for C11 and `employee1`.
- **Expected Result:**
 - A `view` event exists for C11 and `employee1` with a recent timestamp.

TC-3.5: Acknowledge Mandatory Content

- **Related Requirements:** FR-21, FR-22, FR-23
- **Preconditions:** C12 is marked as mandatory for `employee1`.
- **Steps:**
 1. Log in as `employee1` and open C12.
 2. Click **Acknowledge**.
 3. Attempt to call API as a different user to acknowledge C12 on behalf of `employee1`.
- **Expected Result:**
 - Acknowledgement is recorded with timestamp for `employee1`.
 - Attempt to acknowledge on behalf of another user is rejected with an error.

TC-3.6: Content Overview Report Shows Correct Counts

- **Related Requirements:** FR-24
- **Preconditions:**
 - Known numbers of targeted, viewed, and acknowledged users for content C13.
- **Steps:**
 1. As Content Administrator, open Reports Dashboard.
 2. Locate row for C13.
- **Expected Result:**
 - Report displays counts that match the underlying `DeliveryEvent` data.

5.3 Hypothetical Snapshot 3 Test Report

Summary (Hypothetical): All Snapshot 3 tests passed after the date-handling bug from Snapshot 2 was fixed. Reporting metrics align with event data.

Snapshot 3 Test Execution Summary (Hypothetical)

Test Case Group	# Cases	Passed	Failed	Blocked
Targeted Feed (TC-3.1–TC-3.3)	3	3	0	0
Acknowledgements and Events (TC-3.4–TC-3.5)	2	2	0	0
Reporting (TC-3.6)	1	1	0	0
Total	6	6	0	0

6 Snapshot 4 Test Cases: Administration and Regression

6.1 Scope

Snapshot 4 finalizes:

- User and role administration (FR-27–FR-30).
- Regression coverage over previous snapshots.

6.2 Test Cases

TC-4.1: Create New User Account

- **Related Requirements:** FR-27, FR-28

- **Steps:**

1. Log in as System Administrator.
2. Open User Management page.
3. Create a new user with email, name, and role = Employee.
4. Save.

- **Expected Result:**

- New user appears in user list.
- User can log in with initial credentials (after password setup flow, if applicable).

TC-4.2: Deactivate and Reactivate User

- **Related Requirements:** FR-27

- **Steps:**

1. Deactivate existing user `employee3`.
2. Attempt to log in as `employee3`.
3. Reactivate `employee3`.
4. Attempt login again.

- **Expected Result:**

- Deactivated user cannot log in.
- Reactivated user can log in successfully.

TC-4.3: Reset User Password

- **Related Requirements:** FR-29

- **Steps:**

1. As System Administrator, request password reset for `employee4`.
2. Complete reset flow (e.g., admin-set or simulated email token).

3. Attempt login using new password.

- **Expected Result:**

- Login works only with new password.
 - Old password no longer works.

TC-4.4: Audit Log Entry for Administrative Change

- **Related Requirements:** FR-30

- **Steps:**

1. As System Administrator, change the role of `employee4` from Employee to Manager.
2. Open the audit log or administrative change history.

- **Expected Result:**

- Log includes an entry recording who changed which user, from which role to which role, and when.

TC-4.5: Regression – Authentication, Content, and Feed Smoke Test

- **Related Requirements:** FR-01–FR-26 (high-level coverage)

- **Steps:**

1. Log in as employee and verify dashboard loads.
2. Ensure at least one targeted content item appears.
3. Open the content, verify a view event is recorded, and acknowledge if mandatory.
4. As Admin, verify that reporting reflects the new view and acknowledgement.

- **Expected Result:**

- No regressions in core authentication, content visibility, acknowledgement, or reporting paths.

6.3 Hypothetical Snapshot 4 Test Report

Snapshot 4 Test Execution Summary (Hypothetical)

Test Case Group	# Cases	Passed	Failed	Blocked
User and Role Management (TC-4.1–TC-4.4)	4	4	0	0
Regression Smoke Test (TC-4.5)	1	1	0	0
Total	5	5	0	0

Summary (Hypothetical): All Snapshot 4 administration and regression tests passed, indicating the system is ready for final demonstration.

7 Appendix A: Requirement-to-Test Traceability (Partial)

Sample Traceability Between Requirements and Test Cases

Requirement ID	Requirement Summary	Covering Test Case IDs
FR-01	User login with email and password	TC-1.1, TC-1.2, TC-4.5
FR-03	Prevent access when not logged in	TC-1.3
FR-05	Restrict admin pages to roles	TC-1.4
FR-06	Create content items	TC-2.1, TC-2.2
FR-07 & FR-19	Start/end dates and expired content	TC-2.3, TC-3.1
FR-11–FR-14	Targeting rules and updates	TC-2.5, TC-2.6, TC-3.1
FR-15–FR-18	Targeted feed, filters, search	TC-3.1, TC-3.2, TC-3.3
FR-20–FR-23	Views and acknowledgements	TC-3.4, TC-3.5, TC-4.5
FR-24–FR-26	Reporting and exports	TC-3.6, TC-4.5
FR-27–FR-30	User administration and audit logs	TC-4.1–TC-4.4