Customer Requirements Report

Table of Contents

1. Description

My task is to gather requirements and build a secure access management app using the Ruby on Rails framework, with behavior-driven development (BDD) guiding the creation of user stories and scenarios. A lo-fi mockup will outline your app's UI. This report will present project specifics, ensuring clear customer communication.

1.1 Develop UML Diagram for Models

The application consists of four primary models: User, Profile, AccessPoint, and AccessLog, covering a range of data types like String, Enum, DateTime, Integer, and Boolean.

In the UML structure provided, there are:

Models

1. **User**
2. **Profile**
3. **AccessPoint**
4. **AccessLog**

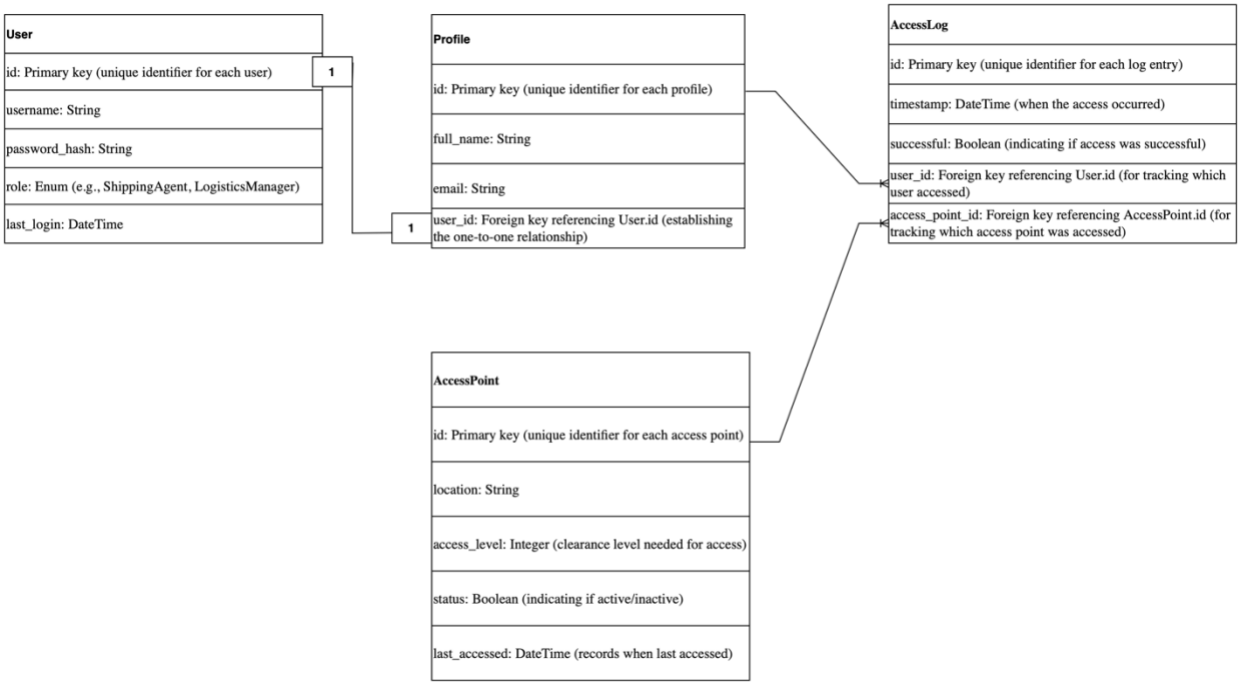
This makes a total of **4 models**.

Data Types

The models use the following data types:

1. **String** (username, password_hash, full_name, email, location)
2. **Enum** (role)
3. **DateTime** (last_login, last_accessed, timestamp)
4. **Integer** (access_level)
5. **Boolean** (status, successful)

This totals **5 different data types** used across the models.



1.2 Create User Stories for Your Web App

General Description:
The secure access management app enables shipping agents to access restricted areas with real-time clearance control, assisting logistics managers in monitoring and auditing access.

Stakeholders:

1. Shipping Agent (user model requiring login and item association).
2. Logistics Manager (can view and search access logs).

User Stories (Connextra Format):

1. As a Shipping Agent, I want to log into the app with secure credentials so that I can access my assigned areas.
2. As a Shipping Agent, I want to view my access history so that I can verify my entry and exit times.
3. As a Logistics Manager, I want to view a log of all agent access attempts so that I can monitor access and track potential issues.
4. As a Logistics Manager, I want to search agent access logs by date and time so that I can audit specific events.

5. As a Shipping Agent, I want to request access to areas outside my clearance level so that I can get supervisor approval if necessary.

User Stories (Refined in Connextra Format)

1. **Secure Login for Access Control**

   - **As a** Shipping Agent
   - **I want** to log into the app with secure credentials
   - **So that** I can access my assigned areas.

2. **Viewing Access History for Self-Verification**

   - **As a** Shipping Agent
   - **I want** to view my access history
   - **So that** I can verify my entry and exit times.

3. **Access Monitoring for Managers**

   - **As a** Logistics Manager
   - **I want** to view a log of all agent access attempts
   - **So that** I can monitor access and track potential issues.

4. **Audit Logs with Search Capability**

   - **As a** Logistics Manager
   - **I want** to search agent access logs by date and time
   - **So that** I can audit specific events.

5. **Requesting Elevated Access for Special Cases**

   - **As a** Shipping Agent
   - **I want** to request access to areas outside my clearance level
   - **So that** I can get supervisor approval if necessary.

1.3 Create BDD Scenarios with Steps

For each user story, create a happy and sad scenario, with error handling in the sad scenarios.

User Story 1: Agent Logs in with Secure Credentials

1. **Scenario 1: Agent successfully logs in (Happy)**

    - **Given** the agent has valid login credentials,
    - **When** they enter their username and password,
    - **Then** they gain access to the dashboard.

2. **Scenario 2: Agent enters incorrect password (Sad)**

    - **Given** the agent has invalid login credentials,
    - **When** they enter an incorrect password,
    - **Then** they receive an "Invalid credentials" message and cannot proceed.

User Story 2: Agent Views Access History

1. **Scenario 1: Agent views access history (Happy)**

    - **Given** the agent is logged in and has previous access history,
    - **When** they navigate to the "Access History" section,
    - **Then** they see a list of all their past entry and exit times.

2. **Scenario 2: Agent has no access history to view (Sad)**

    - **Given** the agent is logged in and has no access history,
    - **When** they navigate to the "Access History" section,
    - **Then** they receive a message saying "No access history available."

User Story 3: Manager Views Agent Access Logs

1. **Scenario 1: Manager successfully views all access logs (Happy)**

    - **Given** the manager is logged in and has permissions to view logs,
    - **When** they access the "Access Logs" page,
    - **Then** they see a complete list of all agent access attempts.

2. **Scenario 2: Manager has restricted access (Sad)**

    - **Given** the manager is logged in but has restricted permissions,

- **When** they attempt to access the “Access Logs” page,
- **Then** they receive an “Access Denied” message.

User Story 4: Manager Searches Access Logs by Date

1. **Scenario 1: Manager searches access logs by a specific date range (Happy)**

   - **Given** the manager is logged in,
   - **When** they enter a specific date range and hit “Search,”
   - **Then** the app displays all access attempts within that date range.

2. **Scenario 2: Manager enters an invalid date range (Sad)**

   - **Given** the manager is logged in,
   - **When** they enter an invalid date range (e.g., start date after end date),
   - **Then** they receive an “Invalid date range” error message and no results are shown.

User Story 5: Agent Requests Access Outside Clearance Level

1. **Scenario 1: Agent successfully requests higher-level access (Happy)**

   - **Given** the agent is logged in and tries to access a restricted area,
   - **When** they request higher clearance level access,
   - **Then** a request is sent to the supervisor for approval, and the agent sees a “Request sent” confirmation message.

2. **Scenario 2: Agent attempts access without permissions and request fails (Sad)**

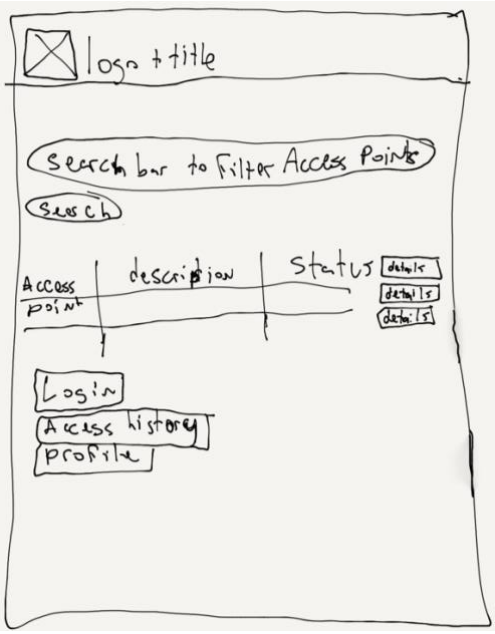
   - **Given** the agent is logged in and tries to access a restricted area without permission,
   - **When** they attempt to request higher clearance but the request fails,
   - **Then** they receive a “Permission request denied” message and cannot access the area.

1.4 Create Lo-Fi UI Mockup

1. Home/Landing Page

Elements:
Search bar to filter access points.
List of available access points with a brief description (e.g., location, status).
Navigation links for login, access history, and profile.

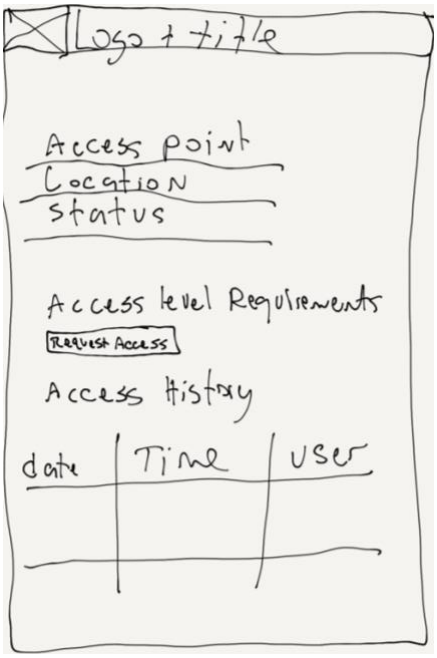
Actions:
View details of an access point by clicking on it.
Use search functionality to filter access points.



2. Access Point Details Page

Elements:
Access point location and status.
Access level requirements.
Button to request access (visible only for Shipping Agent).
List of access history (date, time, user) for that specific point.

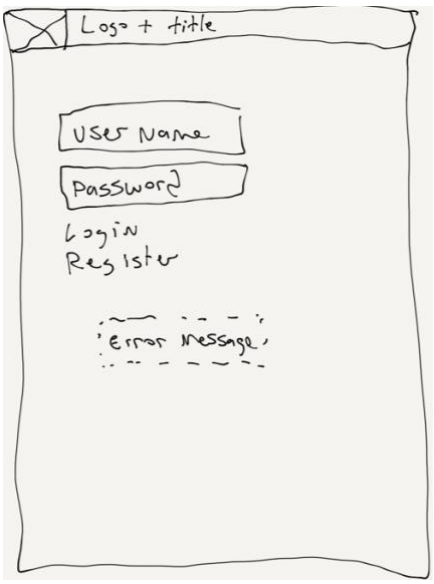
Actions:
Request access if the current user has clearance.
View access logs by clicking on entries.



3. User Registration and Login Page

Elements:
Fields for entering username and password.
Login button and link to register a new account.
Error message placeholder (e.g., “Invalid credentials”).

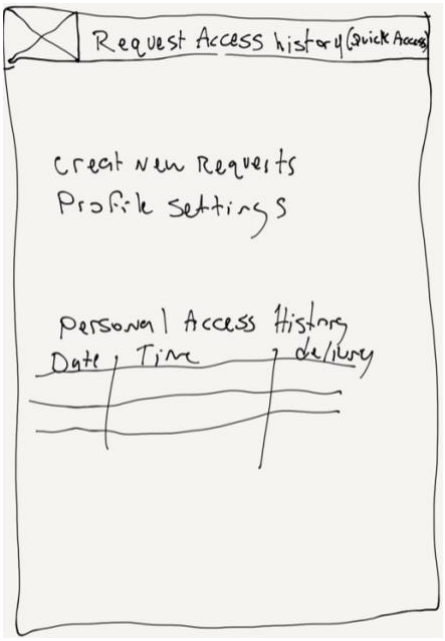
Actions:
Login for existing users.
Registration link redirects to a sign-up page.



4. Agent's Dashboard (Logged-In Home)

Elements:
Quick access to access request history.
Link to create new access requests.
Profile settings.

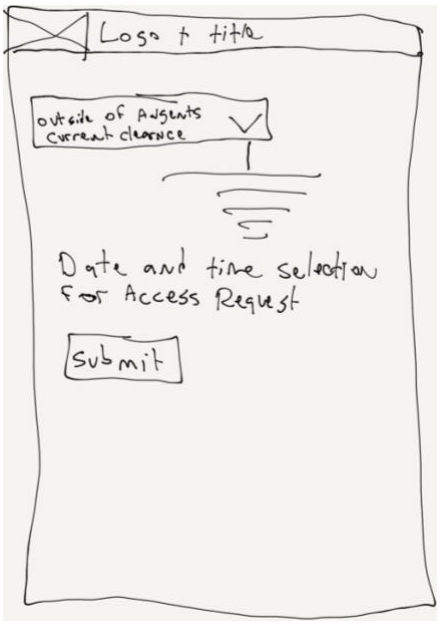
Actions:
Navigate to the access request form.
View personal access history.



5. Create Access Request (Shipping Agent Only)

Elements:
Drop-down list of access points outside the agent's current clearance.
Date and time selection for the access request.
Submit button.

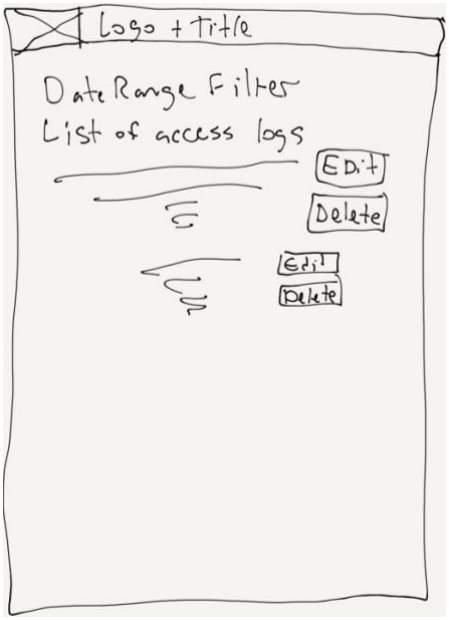
Actions:
Submit access request to supervisor for approval.



6. Access Log Overview (Logistics Manager Only)

Elements:
Date range filter.
List of access logs (user, access point, date, and time).
Edit and delete options for each log entry.

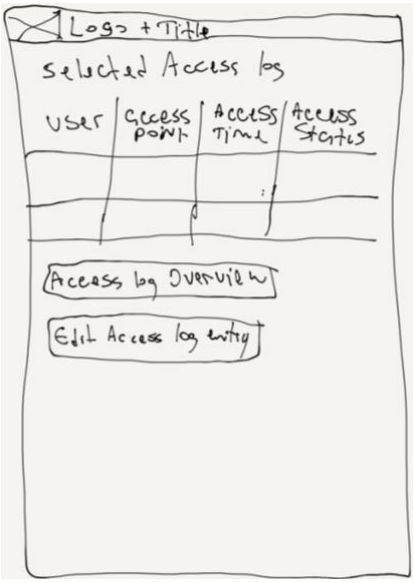
Actions:
Search by date range.
View/edit access logs or delete a specific log entry.



7. Access Log Details Page

Elements:
Detailed view of a selected access log entry (user, access point, access time, access status).

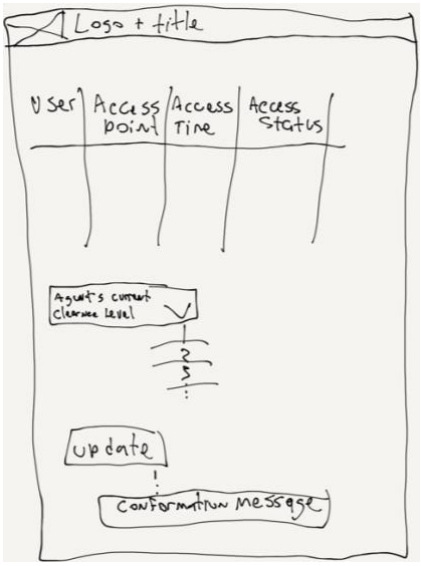
Actions:
Option to return to the Access Log Overview.
Edit access log entry (if permissions allow).



8. Edit Access Clearance (Logistics Manager Only)

Elements:
Form to update clearance level for specific agents.
Drop-down selection of agents and current clearance level.
Submit button for updating clearance.

Actions:
Update clearance level of agents with a confirmation message.



9. Profile Page

Elements:
User information (name, role, last login).
Option to log out or edit profile.

Actions:
Logout button for user.
Option to update profile details.

10. Logout Confirmation Page

Elements:

Simple page asking to confirm logout.

Actions:
Confirm or cancel logout action.