Use Cases

for

Fantastic 6 (F6) Direct Online Store

**Version 1.0 approved**

**Prepared by Fulya Kocaman, Wangmo Tenzing, Vamshi Katipally, Abram Flores, Anthony Hernandez, Manthan Vasani**

**CPSC 541**

**4/24/2022**

**Revision History**

| **Name** | **Date** | **Reason For Changes** | **Version** |
| --- | --- | --- | --- |
| Manthan Vasani | 04/24/2022 | Created | 1.0 |
|  |  |  |  |

## 

## Use Case ID and Name

Id and name: UC-02: Login, Register activity for Admin

## Author and Date Created

Created by: Manthan Vasani Date Created: 04/25/2022

## Primary and Secondary Actors

Primary Actor: Admin Secondary Actor: Developer Team

## Trigger

Activity triggers when Admin clicks on the Sign in or Sign up button.

## Description

Whenever an administrator wants to manage orders, accessing any confidential information, he/she needs to sign into his/her account. If the admin does not have any account he/she needs to create over there. To sign into the account, it requires credentials such as email address and password. For signup the admin has to fill up the form where he/she needs to enter some details like email address, phone no, password, date of birth, address, social security number etc.

## Preconditions

PRE-1: Admin clicks on Sign in or Sign up buttons.

PRE-2: Admins’ identity has been authenticated for sign in activity.

PRE-3: Admin entered all required information for sign up activity.

## Postconditions

POST-1: Admin panel has been displayed after successful authentication.

POST-2: Admin log has been created and added into database with timing and ip address after successful authentication.

POST-3: User ip has been blocklisted after 3 unsuccessful login attempts. Data has been added into the database.

POST-4: Admin details with credentials have been stored into the database after successful signup.

## Normal Flow

1. Admin click on sign in or sign up to access the admin dashboard.
2. Existing admin account holders enter email id and password to access the dashboard by passing two factor authentication.
3. Admin will be redirected to the two factor authentication page.
4. New admin clicks on the Sign up button.
5. Enters required details like first name, last name, email id, password, date of birth, address etc.
6. For new admin account creators, users need to verify email id within a specific time limit.

## Alternative Flows

1. Login session time-out.

Existing admin enters login email and passwords and after the credential verification, admin is redirected to the two factor authentication page.

After the mentioned timeline, if the admin is not able to verify one time password, then the session times out.

1. Email verification link expires

New admin enters all required information into the sign up form.

Admin gets an verification email which contains an “verification link” to the mentioned email id.

Verification link expires within a specific time limit.

If it expires, return to the step 5 of normal flow.

If verification is successful, return to the step 2 of normal flow.

## Exceptions

Unsuccessful login attempts:

1. F6 Direct Online Store System displays admins that they reach the maximum number of attempts during logging in to the admin panel.
2. F6 Direct Online Store System blocks users ip address after reaching the maximum number of invalid login attempts.

## Priority

High

## Frequency of Use

Approximately, 5 users, an average of 1 usage in a week.

## Business Rules

None.

## Other Information

1. Admin shall be able to deny activation of two factor authentication.
2. After reaching maximum invalid login attempts, users’ ip will be blocked and can be unblocked by a database administrator or developer.
3. Admin should get an email after successful account creation.
4. Admin should get an email after every successful and unsuccessful login attempts with timing, location and ip address.

## Assumptions

Assume that the user has access to reliable internet and a device to get connected to the F6 Direct Online Store’s website.

Use Case List

| ***Primary Actor*** | ***Use Cases*** |
| --- | --- |
| Admin | Sign in/ Sign up for admin account |
|  |  |
|  |  |
|  |  |

Use Case Template

| UC ID and Name: | UC-02: Login, Register activity for Admin | | |
| --- | --- | --- | --- |
| Created By: | Manthan Vasani | Date Created: | 04/25/2022 |
| Primary Actor: | Admin | Secondary Actors: | Developer Team |
| Trigger: | Admin clicks on the Sign in or Sign up button. | | |
| Description: | Whenever an administrator wants to manage orders, accessing any confidential information, he/she needs to sign into his/her account. If the admin does not have any account he/she needs to create over there. To sign into the account, it requires credentials such as email address and password. For signup the admin has to fill up the form where he/she needs to enter some details like email address, phone no, password, date of birth, address, social security number etc. | | |
| Preconditions: | 1. PRE-1: Admin clicks on Sign in or Sign up buttons. 2. PRE-2: Admins’ identity has been authenticated for sign in activity. 3. PRE-3: Admin entered all required information for sign up activity. | | |
| Postconditions: | 1. POST-1: Admin panel has been displayed after successful authentication. 2. POST-2: Admin log has been created and added into database with timing and ip address after successful authentication. 3. POST-3: User ip has been blocklisted after 3 unsuccessful login attempts. Data has been added into the database. 4. POST-4: Admin details with credentials have been stored into the database after successful signup. | | |
| Normal Flow: | 1. Admin click on sign in or sign up to access the admin dashboard. 2. Existing admin account holders enter email id and password to access the dashboard by passing two factor authentication. 3. Admin will be redirected to the two factor authentication page. 4. New admin clicks on the Sign up button. 5. Enters required details like first name, last name, email id, password, date of birth, address etc. 6. For new admin account creators, users need to verify email id within a specific time limit. | | |
| Alternative Flows: | 1. Login session time-out.   Existing admin enters login email and passwords and after the credential verification, admin is redirected to the two factor authentication page.  After the mentioned timeline, if the admin is not able to verify one time password, then the session times out.   1. Email verification link expires   New admin enters all required information into the sign up form.  Admin gets an verification email which contains an “verification link” to the mentioned email id.  Verification link expires within a specific time limit.  If it expires, return to the step 5 of normal flow.  If verification is successful, return to the step 2 of normal flow. | | |
| Exceptions: | 1. Unsuccessful login attempts:   1.1: F6 Direct Online Store System displays admins that they reach the maximum number of attempts during logging in to the admin panel.  1.2: F6 Direct Online Store System blocks users ip address after reaching the maximum number of invalid login attempts. | | |
| Priority: | High | | |
| Frequency of Use: | Approximately, 5 users, an average of 1 usage in a week. | | |
| Business Rules: | None | | |
| Other Information: | 1. Admin shall be able to deny activation of two factor authentication. 2. After reaching maximum invalid login attempts, users’ ip will be blocked and can be unblocked by a database administrator or developer. 3. Admin should get an email after successful account creation. 4. Admin should get an email after every successful and unsuccessful login attempts with timing, location and ip address. | | |
| Assumptions: | Assume that the user has access to reliable internet and a device to get connected to the F6 Direct Online Store’s website. | | |