
Pentominoes

HeartSteal
Use-Case Specification: Log In (Admin)

Version 1.0

HeartSteal	Version: 1.0
Use-Case Specification: Log In (Admin)	Date: 18/07/2025

Revision History

Date	Version	Description	Author
18/07/2025	1.0	Initial version	Lưu Vĩnh Phát

HeartSteal	Version: 1.0
Use-Case Specification: Log In (Admin)	Date: 18/07/2025

Table of Contents

1. Use-Case Introduction	4
1.1 Brief Description	4
1.2 Primary Actor	4
2. Flow of Events	4
2.1 Basic Flow	4
2.2 Alternative Flows	4
2.2.1 Invalid information (From step 1)	4
3. Special Requirements	4
4. Preconditions	4
5. Postconditions	4
6. Prototype	5

HeartSteal	Version: 1.0
Use-Case Specification: Log In (Admin)	Date: 18/07/2025

Use-Case Specification: Log In (Admin)

1. Use-Case Introduction

1.1 Brief Description

This use case describes how an authorized administrative user (Admin) authenticates into the system's administrative portal. The Admin supplies credentials and must successfully pass all required security controls (e.g., password, multi-factor authentication, account status checks). Upon success, the Admin is granted an authenticated session with elevated privileges and is redirected to the Admin Dashboard.

1.2 Primary Actor

Administrator

2. Flow of Events

2.1 Basic Flow

1. The administrator launches the application and selects the "Admin Login" option.
2. The system displays the admin login screen with fields for username and password.
3. The administrator enters valid credentials and clicks the "Log In" button.
4. The system validates the entered credentials against the admin user database.
5. The system grants access to the admin dashboard.

2.2 Alternative Flows

2.2.1 Invalid information (From step 1)

1. If the entered credentials are incorrect, the system displays an error message:
"Invalid username or password."
2. The administrator can attempt to log in again or click "Forgot Password."

3. Special Requirements

- The admin login screen must respond within 1 second after the "Log In" button is clicked.
- All passwords must be stored using secure hashing algorithms (e.g., bcrypt or Argon2).
- Support for Two-Factor Authentication (2FA) is mandatory for admin accounts.
- The session for an admin user must time out after 10 minutes of inactivity.

4. Preconditions

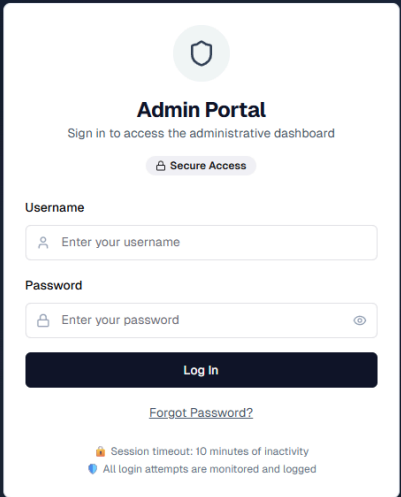
- The administrator account must exist and be active in the system.
- The system is operational and connected to the authentication service.

5. Postconditions

- The administrator is granted access to the admin dashboard with full privileges.
- The system logs the failed login attempt and maintains account security protocols.

HeartSteal	Version: 1.0
Use-Case Specification: Log In (Admin)	Date: 18/07/2025

6. Prototype



The image shows a prototype of an Admin Portal login form. The form is centered on a dark blue background. It features a shield icon at the top, followed by the title "Admin Portal" and the instruction "Sign in to access the administrative dashboard". Below this is a "Secure Access" button. The form includes fields for "Username" and "Password", each with a placeholder text "Enter your username" and "Enter your password" respectively. A "Log In" button is positioned below the password field. At the bottom, there is a "Forgot Password?" link and two status messages: "Session timeout: 10 minutes of inactivity" and "All login attempts are monitored and logged".