# Pentominoes

# HeartSteal
# Use-Case Specification: Log In (Admin)

**Version 1.0**

# Revision History

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

# Table of Contents

# 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.

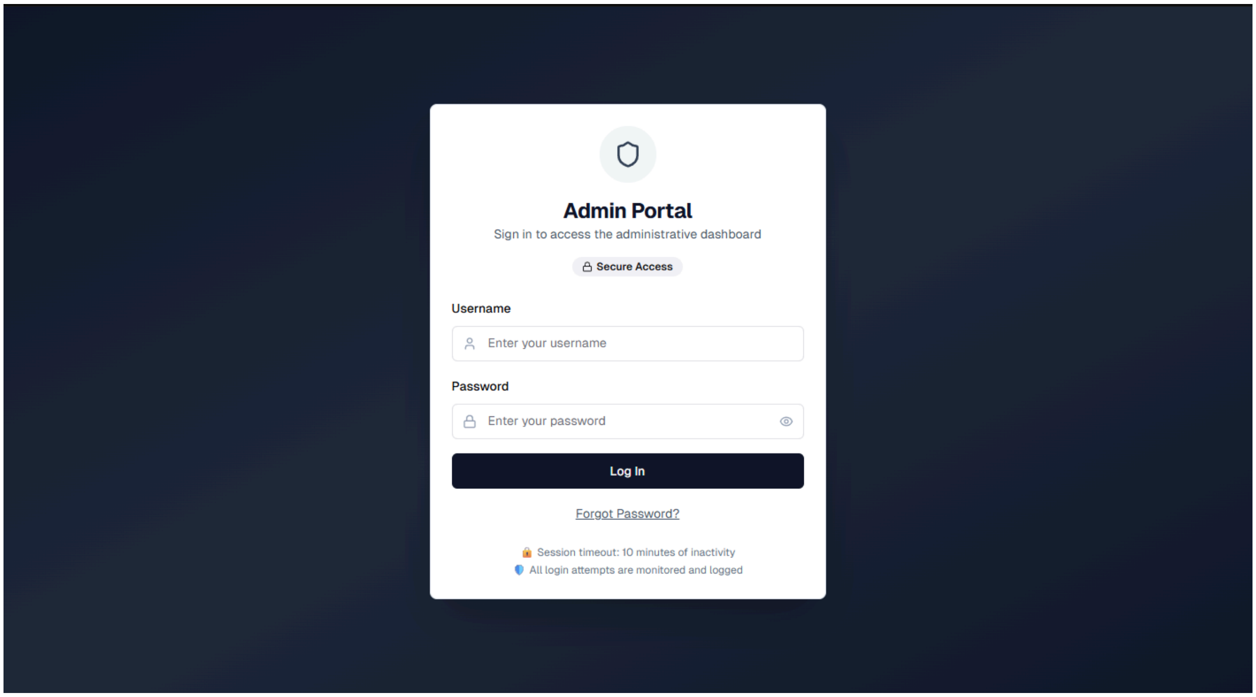
## 4. Preconditions

- 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.

## 6. Prototype



Admin Portal

Sign in to access the administrative dashboard

Session timeout: 10 minutes of inactivity

All login attempts are monitored and logged