# Use Case Specification: Login to System

## Basic Information

| Field | Value |
|---|---|
| **Use Case ID** | UC-AUTH-01 |
| **Use Case Name** | Login to System |
| **Primary Actor** | Patient, Doctor, Nurse, Administrator |
| **Secondary Actors** | System (Authentication Service, Audit Logger) |
| **Brief Description** | Allows an authorized user to authenticate into the NextGenHealth system using email and password. On successful login, a secure session is established. |
| **Priority** | High (Mandatory for all protected operations) |
| **Status** | Proposed / In Analysis |
| **Module** | Authentication and Access Control |
| **Related Requirements** | REQ-AUTH-001, REQ-AUTH-002, REQ-AUTH-003, REQ-SEC-003, REQ-USE-002 |

---

## Preconditions

1. The user has an active account in the system (registered).
2. The user knows their registered email and password.
3. Internet connection is available.
4. Authentication service is operational.

---

## Postconditions

1. On success: User is authenticated and granted access to the system based on their role.
2. A secure session is created (JWT token issued).
3. Session timeout is set (30 minutes of inactivity).
4. Login attempt is logged in the audit trail.
5. On failure: No session is created; user remains unauthenticated.

---

## Main Success Scenario (Basic Flow)

| Step | Actor | System |
|---|---|---|
| 1 | — | Displays login form (email, password, "Login" button). |
| 2 | User | Enters registered email and correct password. |
| 3 | User | Clicks "Login". |
| 4 | System | Validates email format and checks if user exists. |
| 5 | System | Verifies password using secure hash comparison. |
| 6 | System | Checks if account is locked (e.g., after 5 failed attempts). |
| 7 | System | If valid, generates a secure session token (JWT). |
| 8 | System | Sets session timeout to 30 minutes of inactivity. |

| | | |
|---|---|---|
| 9 | System | Logs successful login in audit trail (timestamp, IP, user role). |
| 10 | System | Redirects user to dashboard based on role (Patient Portal, Doctor View, Admin Panel). |

---

# Alternative Flows

## A1 – Invalid Email or Password

- **Trigger**: Step 5 – Credentials do not match.
- **Steps**:
    1. System displays message: "Invalid email or password. Please try again."
    2. Increments failed login counter.
    3. Returns to login form.
- **Resume**: User may retry.
- **After 5 failures**: Account is locked (see E1).

## A2 – Remember Me Option

- **Trigger**: User checks "Remember Me" before login.
- **Modification**:
    - Step 8: Session timeout is extended (e.g., 7 days for trusted devices).
    - Persistent cookie is set (secure, HttpOnly).
- **Security Note**: Not available for administrator accounts.

---

# Exception Flows

## E1 – Account Locked After Failed Attempts

- **Trigger**: 5 consecutive failed login attempts.
- **Steps**:
    1. System locks the account.
    2. Displays message: "Account locked due to multiple failed attempts. Contact administrator or try again in 15 minutes."
    3. Logs event in audit trail.
- **Recovery**:
    - Automatic unlock after 15 minutes, or
    - Manual unlock by administrator.

## E2 – Suspicious Activity Detected

- **Trigger**: Multiple failed logins from different locations/IPs.
- **Steps**:
    1. System flags account for review.
    2. May require additional verification (future: 2FA or email confirmation).
    3. Alert sent to administrator.
- **Note**: Out of scope for initial version, but planned.

## E3 – System or Database Unavailable

- **Trigger**: Step 4 or 5 – Authentication service failure.
- **Steps**:
    1. System logs error.
    2. Displays message: "Service unavailable. Please try again later."
    3. No authentication occurs.
- **End**: Process aborted.

---

## Business Rules

- **BR-AUTH-01**: Maximum of 5 failed login attempts before account lockout.
- **BR-AUTH-02**: Session timeout after 30 minutes of inactivity (REQ-AUTH-002).
- **BR-AUTH-03**: JWT tokens must be securely signed and short-lived.
- **BR-AUTH-04**: Administrator accounts require 2FA (REQ-AUTH-003) — implemented in next iteration.
- **BR-AUTH-05**: "Remember Me" not allowed for administrator roles.

---

## Non-Functional Requirements

| ID | Requirement |
|---|---|
| REQ-PERF-002 | Login page must load in less than 2 seconds. |
| REQ-SEC-002 | All authentication traffic must use TLS 1.3+. Passwords never stored in plain text. |
| REQ-SEC-003 | All login attempts (success/failure) must be logged in audit trail. |
| REQ-USE-005 | Error messages must be clear and not reveal system details (e.g., avoid "User not found"). |
| REQ-REL-001 | System must support 99.9% availability during business hours. |

---

## Data Dictionary (Key Fields)

| Field | Type | Required | Validation |
|---|---|---|---|
| Email | String (100) | Yes | Valid email format |
| Password | String | Yes | At least 8 characters (validated on server) |
| Remember Me | Boolean | No | Optional checkbox |

---

## Notes and Open Issues

- □ Future enhancement: Support Two-Factor Authentication (2FA) for all roles — currently mandatory only for administrators (REQ-AUTH-003).
- □□ HIPAA/GDPR: All login events are auditable and retained for 3+ years (REQ-DATA-002).
- □□ Responsive design: Login form must work on desktop, tablet, and mobile devices (REQ-USE-002).