

**eZ-Audit**  
**Use-Case Specification 3: Login to System**

**Version 1.1**

eZ-Audit	Version: 1.1
Use-Case Specification 3: Login to System	Date: 08/05/2002
Use Case 3	

## Revision History

Date	Version	Description	Author
07/17/2002	1.0	Final version created for 7/17 Deliverable submission	Matt Portolese
08/05/2002	1.1	Revised version created for deliverable re-submission	Matt Portolese

eZ-Audit	Version: 1.1
Use-Case Specification 3: Login to System	Date: 08/05/2002
Use Case 3	

## Table of Contents

1.	Login to the system	4
1.1	Brief Description	4
2.	Flow of Events	4
2.1	Basic Flow	4
2.2	Alternative Flows	5
2.2.1	First time login.	5
2.2.2	Invalid username	5
2.2.3	Invalid Password	5
2.2.4	Invalid password entered 3 times	6
2.2.5	All required fields for login not filled in	7
3.	Special Requirements	7
4.	Preconditions	7
4.1	User must already be registered.	7
4.2	Authentication	7
5.	Postconditions	7
5.1	First time entry	7
5.2	Regular entry	7
6.	Extension Points	8
6.1	Use Case 5 “Change Password”	8
6.2	Use Case 1 “Manage Users”	8
6.3	Use Case 2 “View Submissions”	8
6.4	Use Case 15 “Select an Institution”	8
6.5	Use Case 13 “Assign Submissions”	8
7.	Requirements	8

eZ-Audit	Version: 1.1
Use-Case Specification 3: Login to System	Date: 08/05/2002
Use Case 3	

# Use-Case Specification 3: Login to System

## 1. Login to the system

### 1.1 Brief Description

Every user will be required to login to the system.

## 2. Flow of Events

### 2.1 Basic Flow

1) **General user actor selects the link for the eZ-audit application from the FSA home page or types the URL: <http://www.eZ-Audit.ed.gov> into their browser.**

2) **System presents the login page.**

The user is shown a page with the heading eZ-Audit Login. The following text should immediately follow the heading:

“Welcome to the eZ-Audit website. If this is your first time using this site, you will need a username and temporary password already registered from FSA. If you have visited this site before, please enter your username and password below to login.”

The system will display a username and password label and text boxes for login. A button will also be displayed with the label “Login”.

The following text must also be displayed on the page:

“To reset your password if you have forgotten it, please contact your Administrator during business hours or the Help Desk for after hours support at (202) 555 – 5555 to reset your password.”

“Disclaimer: This site uses cookies. If your browser does not allow cookies, or you do not have cookies enabled, you will not be able to access this site. Please consult the help reference on your browser for the steps to enable cookies.”

3) **The General User actor submits his/her information for authentication.**

The General User actor enters his/her username and password into the appropriate fields and clicks the login button.

4) **The System authenticates the user.**

The system locates the username in the LDAP database and retrieves the profile information using ITA’s available login classes. The system then compares the entered password with the password in the profile to obtain a match. The system sets a flag to true in the session object stating that the user is authenticated. If the user leaves the workstation for 15 minutes, the session object will expire and the flag set to false.

5) **The System presents the home page to the user.**

The appropriate home page is displayed.

eZ-Audit	Version: 1.1
Use-Case Specification 3: Login to System	Date: 08/05/2002
Use Case 3	

## 2.2 Alternative Flows

### 2.2.1 First time login.

Steps 1-4 are the same for the alternate use cases. Only the following steps will change.

**5) The System presents the user the New User Profile page.**

The new user profile page is presented to the user. See extension point – Use Case 5 “Change Password”.

### 2.2.2 Invalid username

Steps 1-2 are the same for the alternate use cases. Only the following steps will change.

**3) The General User actor submits his/her information for authentication.**

The General User actor enters incorrect username and correct password into the appropriate fields and clicks the login button.

**4) The System attempts to authenticate the user.**

The system attempts to locate the username in the LDAP database. The username entered cannot be located.

**5) The System displays the correct message.**

The system redisplay the login welcome page with the following message in red above the username and password entry boxes:

“The username or password you entered is incorrect, please try again.”

**6) The General User actor submits his/her information for authentication.**

The General User actor enters correct username and password into the appropriate fields and clicks the login button.

**7) The System authenticates the user.**

The system locates the username in the LDAP database and retrieves the profile information using ITA’s available login classes. The system then compares the entered password with the password in the profile to obtain a match. The system sets a flag to true in the session object stating that the user is authenticated. If the user leaves the workstation for 15 minutes, the session object will expire and the flag set to false.

**8) The System presents the home page to the user.**

The appropriate home page is displayed.

### 2.2.3 Invalid Password

Steps 1-2 are the same for the alternate use cases. Only the following steps will change.

**3) The General User actor submits his/her information for authentication.**

The General User actor enters correct username and incorrect password into the appropriate fields and clicks the login button.

**4) The System attempts to authenticate the user.**

The system locates the username in the LDAP database and retrieves the profile information using ITA’s available login classes. The system then compares the entered password with the password in the profile to obtain a match. The system sets a flag to false indicating that the password did not match and the user is not authenticated.

**5) The System displays the correct message.**

eZ-Audit	Version: 1.1
Use-Case Specification 3: Login to System	Date: 08/05/2002
Use Case 3	

The system redisplay the login welcome page with the following message in red above the username and password entry boxes:

“The username or password you entered is incorrect, please try again.”

**6) The General User actor submits his/her information for authentication.**

The General User actor enters a correct username and correct password into the appropriate fields and clicks the login button.

**7) The System authenticates the user.**

The system locates the username in the LDAP database and retrieves the profile information using ITA’s available login classes. The system then compares the entered password with the password in the profile to obtain a match. The system sets a flag to true in the session object stating that the user is authenticated. If the user leaves the workstation for 15 minutes, the session object will expire and the flag set to false.

**8) The System presents the home page to the user.**

The appropriate home page is displayed.

**2.2.4 Invalid password entered 3 times**

Steps 1-2 are the same for the alternate use cases. Only the following steps will change.

**3) The General User actor submits his/her information for authentication.**

The General User actor enters correct username and incorrect password into the appropriate fields and clicks the login button.

**4) The System attempts to authenticate the user.**

The system locates the username in the LDAP database and retrieves the profile information using ITA’s available login classes. The system then compares the entered password with the password in the profile to obtain a match. The system sets a flag to false indicating that the password did not match and the user is not authenticated.

**5) The System displays the correct message.**

The system redisplay the login welcome page with the following message in red above the username and password entry boxes:

“The username or password you entered is incorrect, please try again.”

-Repeat steps 3-5 1 time

**6) The General User actor submits his/her information for authentication.**

The General User actor enters a correct username and incorrect password into the appropriate fields and clicks the login button for the third straight time.

**7) The System attempts to authenticate the user.**

The system locates the username in the LDAP database and retrieves the profile information using ITA’s available login classes. The system then compares the entered password with the password in the profile to obtain a match. The system sets a flag to false indicating that the password did not match and the user is not authenticated. The system sets a timeout flag and the current time in the database indicating that the username is locked. If the user tries to login again during this time period, the username will show up as locked and they will not be allowed access.

After 30 minutes, if an attempt is made to login, the username will no longer be locked and may begin at step 1 in the process.

eZ-Audit	Version: 1.1
Use-Case Specification 3: Login to System	Date: 08/05/2002
Use Case 3	

**8) The System displays the correct message.**

The system redisplay the login welcome page with the following message in red above the username and password entry boxes:

“After 3 unsuccessful attempts, your username has been locked. Please contact you administrator for more information.

*2.2.5 All required fields for login not filled in*

Steps 1-2 are the same for the alternate use cases. Only the following steps will change.

**3) The General User actor submits his/her information for authentication.**

The General User actor leaves the username, password field or both blank.

**4) The System displays the correct message.**

The system displays a pop-up box that says the following:

“All fields are required to continue processing, please try again.”

**5) The General User clicks the “OK” button on the pop-up box.**

**6) The System returns the user to the login page.**

The username and password fields are set to blank if information had been entered in either field.

### 3. Special Requirements

No special requirements for this use case.

### 4. Preconditions

**4.1 User must already be registered.**

All users must be registered through the defined registration process. See extension point – Use Case 1 “Manage Users”.

**4.2 Authentication**

- Username: Matches an existing username in the LDAP database
- Password: Matches the password on file in the profile for the username that has been entered.
- Both a username and password have been entered to complete the authentication process.

### 5. Postconditions

**5.1 First time entry**

All users upon the first time entry will be taken to the New User Profile page. See extension point – Use Case 5 “Change Password” for further information.

**5.2 Regular entry**

User will be presented their home page.

- See extension point – Use Case 2 “View Submissions” for information on the external user home page.
- See extension point – Use Case 15 “Select an Institution” for information on the resolution user home page.

eZ-Audit	Version: 1.1
Use-Case Specification 3: Login to System	Date: 08/05/2002
Use Case 3	

- See extension point – Use Case 13 “Assign Submissions” for information on the co-team leader user home page.

## 6. Extension Points

### 6.1 Use Case 5 “Change Password”

Describes the change password functionality for any user.

### 6.2 Use Case 1 “Manage Users”

Describes how an administrator manages users for which they are responsible.

### 6.3 Use Case 2 “View Submissions”

Describes the home page of the external user.

### 6.4 Use Case 15 “Select an Institution”

Describes the home page of the resolution user.

### 6.5 Use Case 13 “Assign Submissions”

Describes the home page of the co-team leader.

## 7. Requirements

- GEN8 The system will provide a Login Page for all users with fields to capture the User’s Username and Password
- GEN9 The system will require a user to enter the correct username and password.
- GEN10 The system will reject a user who enters the wrong username.
- GEN11 The system will reject a user who enters the wrong password.
- GEN12 The system will reject a user who leaves the username blank.
- GEN13 The system will reject a user who leaves the password blank.
- GEN14 The system will verify each user's username and password prior to authorization to the system.
- GEN20 The system will support ED password syntax rules and management rules.
- GEN23 The system will support rules that enforce the following capabilities:· Password expires on the first logon attempt for a new user· Password uniqueness set to 5 - i.e., systems stores and recalls past 5 passwords· Automatic account lockout after 3 unsuccessful login attempts· Set Account Lockout button· Automatic log-out duration set to 30 minutes of inactivity - validate with session management req· Unsuccessful login counter reset to 0 from 3 after 30 minutes
- GEN24 The system will store passwords in an encrypted state in the credential repository.
- GEN1201 The System will encrypt user passwords and other sensitive data in the LDAP and Oracle DBs
- GEN1202 The System security will support user authentication by implementing user IDs and passwords
- GEN100 The system will provide each Ed user (Audit Resolution Specialist, Financial Analyst and Co-Team leader) with ability to update his/her name on the Admin Profile page.
- GEN101 The system will provide each Ed user (Audit Resolution Specialist, Financial Analyst and Co-Team leader) with ability to update his/her Email address on the Admin Profile page.
- GEN102 The system will provide each Ed user (Audit Resolution Specialist, Financial Analyst and Co-

eZ-Audit	Version: 1.1
Use-Case Specification 3: Login to System	Date: 08/05/2002
Use Case 3	

- Team leader) with ability to update his/her phone number on the Admin Profile page.
- GEN103 The system will provide each Ed user (Audit Resolution Specialist, Financial Analyst and Co-Team leader) with ability to update his/her fax number on the Admin Profile page.