

**eZ-Audit**  
**Use-Case Specification 5: Change Password**

**Version 1.1**

eZ-Audit	Version: 1.1
Use-Case Specification 5: Change Password	Date: 08/05/2002
Use Case 5	

## 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 5: Change Password	Date: 08/05/2002
Use Case 5	

## Table of Contents

1.	First Time Login	4
1.1	Brief Description	4
2.	Flow of Events	4
2.1	Basic Flow	4
2.2	Alternative Flows	5
2.2.1	User updates profile information and password.	5
2.2.2	Password in wrong format	5
2.2.3	New password and re-typed new password did not match	5
2.2.4	Password expired	6
3.	Special Requirements	7
4.	Preconditions	7
4.1	User must be logged in.	7
5.	Postconditions	7
5.1	User continues to home page.	7
6.	Extension Points	7
6.1	Use Case 3 “Login to System”	7
6.2	Use Case 2 “View Submissions”	7
6.3	Use Case 15 “Select an Institution”	7
6.4	Use Case 13 “Assign Submissions”	7
7.	Validations	7
8.	Requirements	7

eZ-Audit	Version: 1.1
Use-Case Specification 5: Change Password	Date: 08/05/2002
Use Case 5	

# Use-Case Specification 5: Change Password

## 1. First Time Login

### 1.1 Brief Description

Every user will verify their profile information and change their password upon logging into the system for the first time.

## 2. Flow of Events

### 2.1 Basic Flow

#### 1) General user actor successfully logs into the application for the first time.

The system retrieves the information from for the following fields and pre-populates them in the profile page:

- First Name
- Last Name
- Email address
- Office phone
- Office extension
- Fax

#### 2) System presents the “my profile” page with the heading “New User Profile”.

The user is shown a page with the fields listed above and their information from the system pre-populated in text boxes. The system also presents 2 additional fields to be used for changing the password. The following text should be displayed below the page heading and above the previous pre-populated fields:

“Welcome to eZ-Audit. Please take a few moments to review the information we currently have on file and update any incorrect or outdated information.”

The page should then show a new heading, “Change Password” followed by the following text, fields and buttons:

“You will also need to change your password from the temporary password that was assigned to one that you can remember easily. The password must be 8– 15 characters in length and must include at least 3 of the following types of characters: uppercase letters(A-Z), lowercase letters(a-z), numeral values(0-9) and special characters(<, >, ?, \$, etc.). The password must be dissimilar from your previous five passwords.”

Field labels with text boxes:

- New password
- Re-type new password

Buttons:

- Save
- Reset

eZ-Audit	Version: 1.1
Use-Case Specification 5: Change Password	Date: 08/05/2002
Use Case 5	

**3) The General User actor verifies that the profile information is correct and changes their password.**

The General User actor enters the new password and re-types the new password into the appropriate fields. The user then presses the “Save button”

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

A pop-up box appears with the message:

“Your password has now been changed.”

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

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

The appropriate home page is displayed.

## 2.2 Alternative Flows

### 2.2.1 User updates profile information and password.

Steps 1-3 are the same for the alternate use cases. Only the following steps will change.

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

A pop-up box appears with the message:

“Your profile information and password has now been changed.”

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

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

The appropriate home page is displayed.

### 2.2.2 Password in wrong format

Steps 1-3 are the same for the alternate use cases. Only the following steps will change.

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

A pop-up box appears with the message:

“The new password you entered does not meet system requirements. Passwords must be 8– 15 characters in length and must include at least 3 of the following types of characters: uppercase letters(A-Z), lowercase letters(a-z), numeral values(0-9) and special characters(<, >, ?, \$, etc.). The password must be dissimilar from your previous five passwords.”

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

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

The identification fields do not change (first name, last name, email, etc.). The new password and re-type new password fields have been set to blank.

### 2.2.3 New password and re-typed new password did not match

Steps 1-3 are the same for the alternate use cases. Only the following steps will change.

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

A pop-up box appears with the message:

eZ-Audit	Version: 1.1
Use-Case Specification 5: Change Password	Date: 08/05/2002
Use Case 5	

“The new passwords you typed in do not match, please try again.”

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

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

The identification fields do not change (first name, last name, email, etc.). The new password and re-type new password fields have been set to blank.

#### 2.2.4 Password expired

Step 1 is the same for the alternate use cases. Only the following steps will change.

**2) System presents the “my profile” page with the heading “New User Profile”.**

The user is shown a page with the fields listed above and their information from the system pre-populated in text boxes. The system also presents 2 additional fields to be used for changing the password. The following text should be displayed below the page heading and above the previous pre-populated fields:

“Welcome to eZ-Audit. Please take a few moments to review the information we currently have on file and update any incorrect or outdated information.”

The page should then show a new heading, “Change Password” followed by the following text, fields and buttons:

“Your password has expired. Please choose a new password that is easy to remember. The password must be 8– 15 characters in length and must include at least 3 of the following types of characters: uppercase letters (A-Z), lowercase letters(a-z), numeral values(0-9) and special characters(<, >, ?, \$, etc.). The password must be dissimilar from your previous five passwords.”

Field labels with text boxes:

- New password
- Re-type new password

Buttons:

- Save
- Reset

**3) The General User actor verifies that the profile information is correct and changes their password.**

The General User actor enters the new password and re-types the new password into the appropriate fields. The user then presses the “Save button”

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

A pop-up box appears with the message:

“Your password has now been changed.”

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

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

The appropriate home page is displayed.

eZ-Audit	Version: 1.1
Use-Case Specification 5: Change Password	Date: 08/05/2002
Use Case 5	

### 3. Special Requirements

No special requirements for this use case.

### 4. Preconditions

#### 4.1 User must be logged in.

A user must be logged in to change their password.

- See extension point – Use Case 3 “Login to System” for login information.

### 5. Postconditions

#### 5.1 User continues to home page.

If logging in for the first time or for password expiration, the user will continue in the process to their home page. If changing profile information, the user will be returned to the 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.
- 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 3 “Login to System”

Describes the login process.

#### 6.2 Use Case 2 “View Submissions”

Describes the home page of the external user.

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

Describes the home page of the resolution user.

#### 6.4 Use Case 13 “Assign Submissions”

Describes the home page of the co-team leader.

### 7. Validations

- First Name: Alpha; max 20
- Last Name: Alpha; max 30
- Email address: Alphanumeric and @ symbol; format: yourname@school.edu; max 50
- Phone and Fax number: Numeric; format 999-999-9999; max 10
- Password: At least 3 of each: Uppercase alpha, lowercase alpha, numeral values, and special characters(<, >, ?, \$, etc.); minimum 8 characters; maximum 15 characters; dissimilar from previous 5 passwords

### 8. Requirements

- GEN18 The system will support syntax rules that allow the following elements to be incorporated into

eZ-Audit	Version: 1.1
Use-Case Specification 5: Change Password	Date: 08/05/2002
Use Case 5	

passwords:· Alphanumeric values· Alpha-only values· Numeric-only values

- GEN19 The system will support rules that enforce the following capabilities:· Password lifetime from 120 days (ED User)· Unlimited password lifetime (Institution & Audit)· Comparison to 5 previous passwords for the user· Disabling of the account after a period of inactivity of 90 to 365 days
- GEN20 The system will support ED password syntax rules and management rules.
- GEN21 The system will support a minimum password length of 8 characters.
- GEN22 The system will support syntax rules that enforce at least three of the following conditions on every password:· Uppercase alphabetic characters (A-Z)· Lowercase alphabetic characters (a-z)· Numeral values (0-9)· Non-alphabetic and non-numeric characters ( < ! @ # etc.)
- 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.
- GEN70 The system will require passwords to adhere to FSA password syntax rule.