**USE CASE: Change password**

Document History

Document Location

This is a snapshot of an on-line document. Paper copies are valid only on the day they are printed. Refer to the author if you are in any doubt about the currency of this document.

The source of the document will be found …

Revision History

|  |  |  |
| --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes |
| 1.0 | 7/2/2013 | Initial document |
| 1.1 | 7/5/2013 | Revised |
|  |  |  |
|  |  |  |

Approvals

This document requires following approval signature. Signed approval forms are filed in …

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |
|  |  |

Distribution

This document has been distributed to:

|  |  |
| --- | --- |
| **Name** | **Title** |
|  |  |
|  |  |
|  |  |
|  |  |

Contents

1. Introduction 5

1.1 Purpose 5

1.2 References 5

1.3 Notation/Structure 5

2. Use Cases 6

2.1 Use Case Name: Change password 6

2.1.1 Use Case Overview…. 6

# Introduction

Use Cases are detailed descriptions of how users and systems interact with an application. These descriptions include ideal paths with alternate paths and post conditions. This information assists the structure and interface design for the best possible experience for the site’s users. Additionally, the Use Cases are used by the QA team to ensure all objectives and requirements were met and fulfilled successfully.

A set of Use Cases can be created to describe the majority of user interactions with the application. The Use Case will ultimately drive the User Experience team in defining the interface. With a clear distinction between user and system interactions written in use case form the UI can be developed in more detail.

Each Use Case follows and tracks back to business requirements.

## Purpose

This document describes the Use Cases for the outlined system.

Use Cases are used to explore and communicate the likely actions of users and the system when interacting with the application. Development of Use Cases helps the design team understand the business requirements and how they can ultimately drive the design and user experience.

## References

This document is based on the following documents:

* Document Name

## Notation/Structure

Use Cases typically have the following sections:

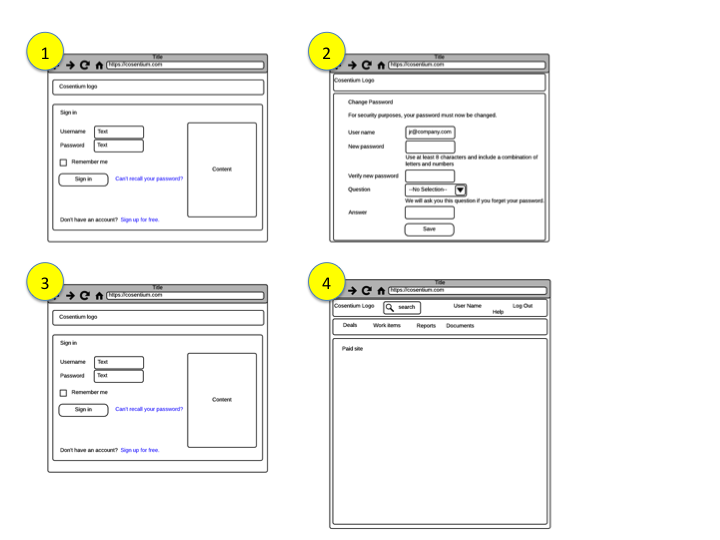
1. Overviews
2. Preconditions
3. Triggers
4. Main Flows
5. Alternate Flows
6. Business Rules
7. Messages (system generated)

# Use Cases

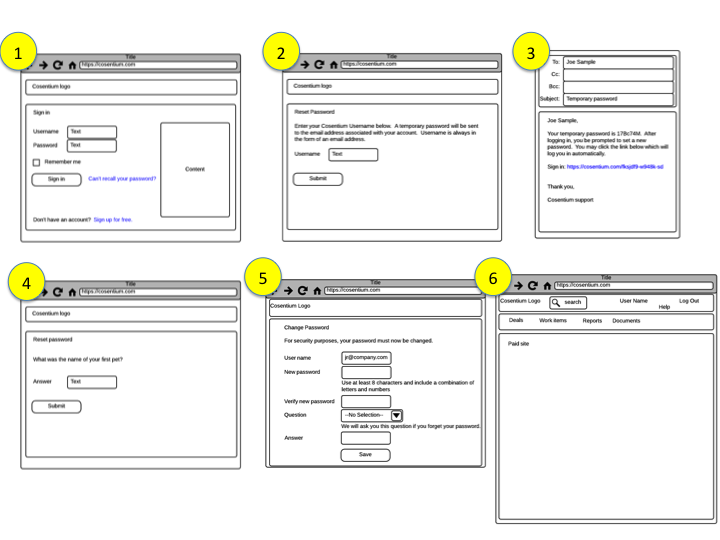
## Use Case Name: Change password

### Use Case Overview….

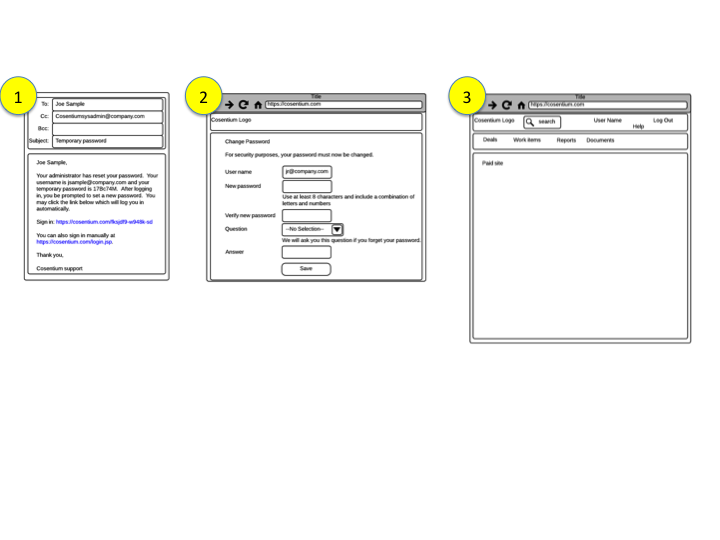
|  |  |  |
| --- | --- | --- |
| **Use Case ID** | **Change password** | |
| **Use Case Overview** | A user may change to a new password on their own, or because system policies require that they change passwords, or because they cannot remember their password. This use case document covers the core case of changing passwords which is common to all of these.  Cosentium customers will desire security features such as strong passwords, account lock out after multiple unsuccessful login attempts, non re-usable passwords, required password changes, session time-outs, two factor authentication, and strong authentication for unrecognized devices. Some of these security requirements manifest themselves in the change password use case.  Authenticated logged in users (just completed login screen with old password and now security policy requires password change, or user initiated password changes from within the system) changing passwords ***are not*** sent a system generated link to their email address as the starting point.  Non-authenticated users changing passwords (lost password, or system admin password resets) ***are*** sent a system generated link to their email address as the starting point. | |
| **Precondition** | 1. User has an account on the system | |
| **Trigger(s)** | 1. Sys admin has pushed the user a password reset message, or.. 2. Logged in user initiates change password sequence (personal setup/change password), or.. 3. User clicks on "lost password" link from the sign in page, or.. 4. User attempts to sign in with expired password | |
|  | | |
| **B - Main Flow- Authenticated User, expired password** | | |
|  | B1 | User accesses sign-in page, uses correct credentials but password has expired.  System displays "Sign in" page. The page includes an entry box for <username> with a label of "Username" next to it (<username> is prefilled if the user has previously checked the "Remember me" box at sign in), an entry box for <password> with a label of "Password" next to it, a checkbox for <remember\_me> with label of "Remember me" next to it (note <remember\_me> checkbox is unchecked by default unless the user has previously checked the checkbox), a button labeled "Sign in" with text "Can't recall your password?" next to it formatted as hypertext, text "Don't have an account?" with hyperlinked text "Sign up for free" next to it.  If user initiates change password sequence from Personal setup/change password, this is Alternate Flow A1.  If user clicks through "Can't recall your password?"" link from the sign-in page, this is Alternate Flow A2.  If system admin pushes the user a password reset message, this is Alternate Flow A3  If user clicks "Sign up for free", this is Alternate Flow A4 |
|  | B2 | User clicks "Sign in"  System does validation as follows:  1. <Username> must match a username existing in the system  2. <Password> must match the password entry in the database for the corresponding user  3. <Password> must not be expired.  If validation fails #1, #2 or both, redisplay B1 with red highlighting next to the field(s) that did not pass validation, along with informative text in red to help the user know how to correct. The field correction help text to be displayed is as follows:  1. If "Username" does not match a username existing in the system, display M4 next to or adjacent to the area where the user enters Username and Password. The red highlighting text should not be specific to the field that failed validation (security precaution).  2. If user makes more than 5 unsuccessful attempts to authenticate, display account locked page saying "You have attempted to login more than 5 times. Your account has been locked for 30 minutes. You can contact your administrator to reset your account or wait until the lock expires and try logging in again." (M5)  If validation passes #1 and #2, but fails #3, proceed to B2  If validation passes #1, #2, and #3 then proceed to B6 |
|  | B3 | Change password page  System displays "Change password" page. The page displays the text, "For security purposes, your password must now be changed." The page displays the following fields: <username> (labeled "Username") with user's username prefilled and viewable but not editable, <new password> (labeled "New Password") and with adjacent text that says "Password must consist of at least 8 characters and include at least one lowercase letter, one uppercase letter, and one special character ", <verify new password> (Labeled "Verify New Password"), <question> (Labeled "Question" and formatted as drop down list) and with adjacent text that says "We will ask you this question if you forget your password", <answer> (Labeled "Answer").  The questions that are available for the user to choose from in the "Question" drop down list are:  - "What city were you born in?"  - "What was the name of your first pet?"  - "What is your mother's middle name?"  - "What is the name of an elementary school you attended?"  The following fields allow and require user entry: <new\_password>, <verify\_new\_password>, <security\_question> (drop down), <security\_question\_answer>.  There is only one button the user can click on, "Save". To abandon, the user must close the page. |
|  | B4 | User clicks "Save"  System does validation as follows:  1. All editable fields must have entries  2. <new password> and <verify new password> must match  3. <new password> must meet security policy requirement (consist of at least 8 characters and include at least one lowercase letter, one uppercase letter, and one special character)  4. <new password> must not match a previously used password for the user.  If field(s) do not have an entry, redisplay B2 with informative M1 text next to the field(s) that are missing entries.  If <new password> and <verify new password> do not match, redisplay B2 with informative M3 text next to the <verify new password> field.  If <new password> is the same as a previously used password, redisplay B2 with informative M8 text next to the <new password> field.  If <new password> does not meet security policy requirement, redisplay B2 with informative M2 text next to the <new password> field. |
|  | B5 | Return user to step B1 |
|  | B6 | Paid Site home page. |
| **Post-**  **conditions** | * Logged in user * Updated user account with new password along with date/time stamp that new password was established * Saved record of old password so it can be checked when new passwords are established (to make sure old passwords are not reused) | |
|  | | |
| **A1** | **Authenticated user initiated password change** | |
|  | A1.1 | User selects Personal Setup/Change Password |
|  | A1.2 | User delivered to A3.1 of Alternate Flow A3 in "use case personal account info 06122013.docx" for details on how this works. |
| **Post-**  **conditions** |  | |
|  | | |
| **A2** | **Non authenticated user clicks "lost password" link** | |
|  | A2.1 | User clicks on "Can't recall your password?" on the sign in page |
|  | A2.2 | Enter your Username page. The page is titled "Reset Password" below which it says, "Enter your Cosentium Username below. A temporary password will be sent to the email address associated with your account. Username is always in the form of an email address." Below these instructions is the label "Username" and an adjacent text entry field. Below these is a button labeled "Submit". |
|  | A2.3 | Submit.  System does validation as follows:  1. Username must be in the form of an email address  2. Username must exist in the system  If validation fails #1, present A2.2 again with informative M9 text adjacent to the Username text entry box.  If validation fails #2, close the page and do not alert the user to any error condition.  If validation passes #1 and #2, close the page |
|  | A2.4 | Receive email with system generated link. The email should come from an alias called "support@cosentium.com", be received on the email address associated with the user account that was entered in step A2.2, and be in plain text format. The email should have the subject line, "Temporary Password". The body of the message should be as follows:  <first\_name> <last\_name>,  Your temporary password is <system generated temporary password>. After logging in, you be prompted to set a new password. You may click the link below which will log you in automatically.  Sign in: <system generated user specific single use login link>  Thank you,  Cosentium support |
|  | A2.5 | Answer security question page. The page is titled "Reset Password". Below the page title the security question associated with the user's account is displayed. Below the question, the text "Answer" is displayed with an adjacent text entry box. Below all of this is a button labeled "Submit". |
|  | A2.5 | Submit  System does validation as follows:  1. The answer provided by the user must match the answer in the database.  If validation fails #1, present A2.5 again with informative M10 text adjacent to the text entry box.  If user makes more than 5 unsuccessful attempts to answer the security question, display an Account Locked page that says "You have attempted to answer the security question more than 5 times. Your account has been locked for 30 minutes. You can contact your administrator to reset your account or wait until the lock expires and try logging in again." |
|  | A2.6 | Deliver user is transported to step B3, main flow (above). |
|  | A2.7 | Paid site |
| **Post-**  **conditions** | * Logged in user * Successfully changed password * Updated user account with new password along with date/time stamp that new password was established | |
|  | | |
| **A3** | **Non authenticated receives reset password message pushed from system admin** | |
|  | A3.1 | Sys admin resets password |
|  | A3.2 | Receive email with system generated link. The email should come from an alias called "support@cosentium.com", be received on the email address associated with the user account in the database, have the company's Cosentium system admin in copy, and be in plain text format. The email should have the subject line, "Temporary Password". The body of the message should be as follows:  <first\_name> <last\_name>,  Your administrator has reset your password. Your username is <username> and your temporary password is <system generated temporary password>. After logging in, you be prompted to set a new password. You may click the link below which will log you in automatically.  Sign in: <system generated user specific single use login link>  You can also sign in manually at https://cosentium.com/login.jsp  Thank you,  Cosentium support |
|  | A3.4 | Click on system generated link in the email, user is transported to step B3, main flow (above)/ |
|  | A3.5 | Paid site |
| **Post-**  **conditions** | * Logged in user * Successfully changed password * Updated user account with new password along with date/time stamp that new password was established | |
|  | | |
| **Messages** | M1 | "You must enter a value" |
|  | M2 | "Passwords must consist of at least 8 characters and include at least one lowercase letter, one uppercase letter, and one special character" |
|  | M3 | "Password entries must match" |
|  | M4 | "Username and password combination does not match our records" |
|  | M5 | "You have attempted to login more than 5 times. Your account has been locked for 30 minutes. You can contact your administrator to reset your account or wait until the lock expires and try logging in again." |
|  | M8 | "Passwords cannot have been used previously" |
|  | M9 | "Username must be in the form of an email address." |
|  | M10 | "Security question answer does not match our records" |
|  | | |
| **BRs** | 1 |  |
|  | 2 |  |
|  | 3 |  |



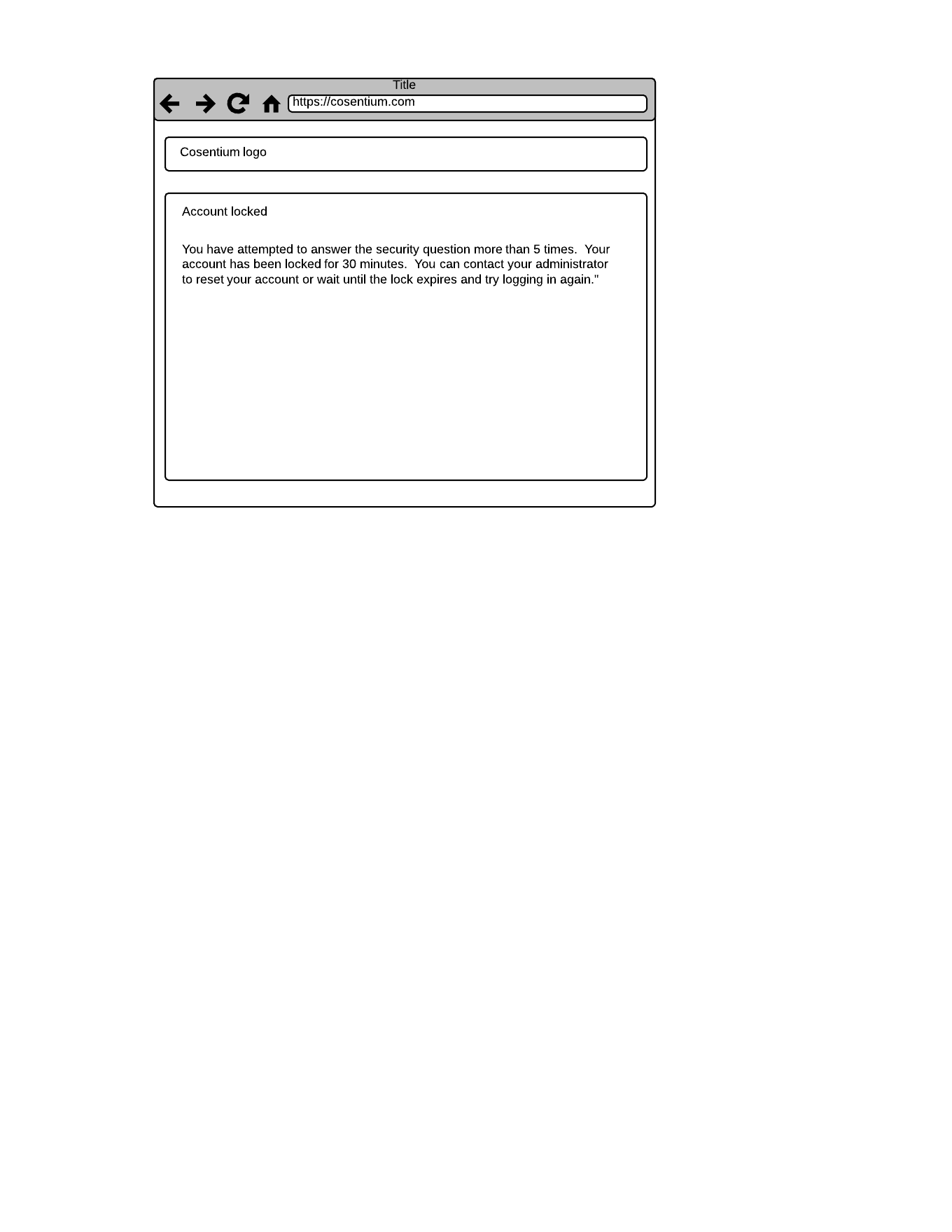
VR1: "Flow for authenticated user password expired.png"



VR2: " Flow for Non Authenticated user cant remember password.png"



VR3: "Flow for Non authenticated receives reset password message pushed from system admin.png"



VR4: "account locked - New Page.png"