CalSAWS

California Statewide Automated Welfare System

Design Document

CA-207220 | DDID 2054

Add Notification message when User exits page without saving

CalSAWS	DOCUMENT APPROVAL HISTORY	
	Prepared By	Erika Kusnadi-Cerezo
	Reviewed By	Amy Gill

DATE	DOCUMENT VERSION	REVISION DESCRIPTION	AUTHOR
03/13/2020	1.0	Initial	Erika Kusnadi-Cerezo
05/04/2020	2.0	Added to the design specifics on what counts as 'Create' and 'Edit' mode and when alert notification will display	Erika Kusnadi-Cerezo
05/13/2020	3.0	Remove 'bn' from the top of page 1. Updated Section 2, 2.1 and 2.1.3 (point#1) to add 'saving or cancelling the change' appropriately to each paragraph.	Erika Kusnadi-Cerezo
5/27/2020	4.0	Updated the title of the design document to DDID 2054 – Add Notification message when User exits page without saving. Added more explanation on why certain pages are not included to display the notification message. Updated the design to be more consistent in using notification message instead of alert.	Erika Kusnadi-Cerezo
6/23/2020	5.0	Remove from the Description of Changes on how the system should behave in the background when the message display and browser functionality is applied.	Erika Kusnadi-Cerezo
7/27/2020	6.0	Updated the Description of Changes #2.a.i to exclude the LRS/CalSAWS homepage from having the notification.	Erika Kusnadi-Cerezo

Table of Contents

1 OVERVIEW

1.1 Current Design

Currently both the C-IV system and LRS/CalSAWS do not have any type of notification when a user makes an update to a page in “Create” or “Edit” mode and then navigates away from the page without using the “Save”, “Cancel”, or other similarly named buttons such as “Save and Add Another” or “Save and Return” button.

1.2 Requests

Update LRS/CalSAWS to display a notification message when users make a change to a page in “Create” or “Edit” mode to confirm whether they would like to stay or leave the page. Message to only display if they are navigating away from the page without going the route of using the “Save”, “Cancel”, or other similar buttons that are part of the page.

1.3 Overview of Recommendations

Update LRS/CalSAWS to display a notification message whenever a user applied changes to a page in “Create” or “Edit” mode but then navigated away from the page prior to saving the changes (i.e., clicking the save button) or navigating away from the page by way of the “Cancel” button.

1.4 Assumptions

1. Existing functionality will remain unchanged with the addition of the notification message being added to all “Create” and “Edit” mode pages.

2 RECOMMENDATIONS

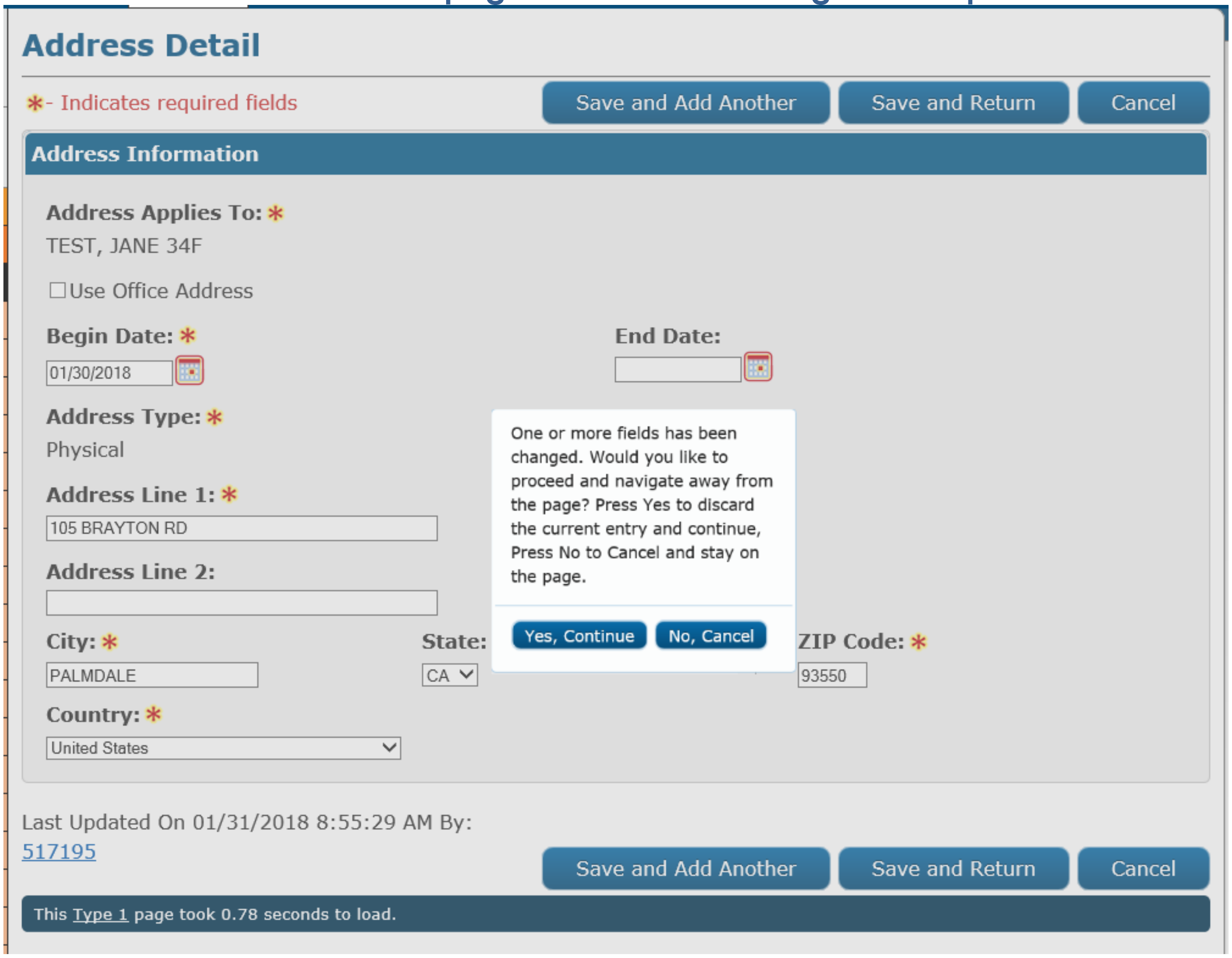
Update the LRS/CalSAWS system to display a notification message to all "Create" and "Edit" mode type page(s), that will ask the user to confirm whether they would like to navigate away from the page without saving or cancelling the change and have the changes be discarded or cancel and stay on the page.

2.1 Update "Create" and "Edit" mode pages

2.1.1 Overview

Update all "Create" and "Edit" mode pages within LRS/CalSAWS to display a notification message that will ask the user to confirm whether they would like to navigate away from the page without saving or cancelling the change and have the changes be discarded or cancel and stay on the page.

2.1.2 "Create" and "Edit" mode page notification message Mockup



Address Applies To: *
TEST, JANE 34F

□ Use Office Address

Begin Date: * 01/30/2018

End Date:

Address Type: * Physical

Address Line 1: * 105 BRAYTON RD

Address Line 2:

City: * PALMDALE

State: CA

ZIP Code: * 93550

Country: * United States

One or more fields has been changed. Would you like to proceed and navigate away from the page? Press Yes to discard the current entry and continue, Press No to Cancel and stay on the page.

Last Updated On 01/31/2018 8:55:29 AM By: 517195

This Type 1 page took 0.78 seconds to load.

Figure 2.1.1 – "Create" and "Edit" mode type page notification message Mockup

2.1.3 Description of Changes

1. Create a notification message that will display when the user makes a change to a page in "Create" or "Edit" mode but then navigates away from the page without saving or cancelling the change. The notification message will display as in Figure 2.1.1.
    a. Message to display on the notification message: "One or more fields has been changed. Would you like to proceed and navigate away from the page? Press Yes to discard the current entry and continue, Press No to Cancel and stay on the page.
    b. Two buttons will be displayed at the bottom of the notification alert and labeled as follows:
        i. Yes, Continue
            1. Clicking this button will take the user to the page that they were trying to navigate to and the changes that were made to the page will be discarded.
        ii. No, Cancel
            1. Clicking this button will keep the user on the current page and changes that were applied will still be displayed the same way prior to the user trying to navigate away.
    c. The page displayed in the background behind the notification message will be greyed out (as shown on figure 2.1.1) and users must take action by clicking on the 'Yes, Continue' button or 'No, Cancel' button on the notification message before the user is able to continue.
2. Notification message will display when the following criteria is met:
    a. User is in a "Create" or "Edit" mode page of the main window in the LRS/CalSAWS system.
        i. This functionality will not be in place for EDBC and EDBC related pages due to these pages being unique and the amount of data being inputted are limited. LRS/CalSAWS homepage since the amount of data being inputted are limited. Pop-up windows such as Audit pages, Document parameters, editable forms, Journal, Task, Call Log, and Reception Log are excluded since workers will need to close out the window in order to navigate away other than clicking the 'Save' button or the 'Cancel' button. Closing the window using the 'X' button will not trigger the notification message since it is browser functionality, not a functionality within the LRS/CalSAWS application.
    b. User made a change to one or more fields on the page then navigated away without applying the change by saving it first by way of the "Save" button or other similar type buttons that apply the changes to the page.
        i. In order for the notification message to display, users must navigate away by the following options:

1. Clicking on one of the available options in the Local navigator.
2. Clicking on one of the available options in the Task navigator.
3. Entering a case number on the "Case Number field" on the Task navigator bar and then clicking "Go".
4. Clicking the "LRS" logo on the top left hand corner to take the user to the home page.
5. Clicking the "Log Out" button on the Utilities navigation bar.

Note: If users navigate away from the page via other methods that are not listed above, the notification message will not display regardless if other criteria/conditions are met that are listed in this design document.

ii. In order for the notification message to display users must apply a change to an editable field within the page in "Create" or "Edit" mode.

Value or information that was inputted into an "Editable" field was updated. This means the value or information does not equal to the value or information from when the page originally loaded to when the user tried to navigate away from the page (navigating away through one of the options listed above).

Note: If the value or information was changed but then changed back to the original value when the page initially loaded, the notification alert will not display.

1. If a user applies a change to an editable field on a page and then navigates away to a child page by using a button or a hyperlink within the page (this will not trigger the notification message since the user did not navigate away from the page by using one of the option listed above), and then returns to the original page, the notification message will not display if the user does not make any other changes to an editable field at that point and navigates away by using one of the options listed above.

   Example: User updated an editable field on the 'Income Detail' page then navigated to the 'Income Amount Detail' page, and then returned to the 'Income Detail' page. If the user did not make another change to an editable field at this point, the notification message will not display when they navigate away from the 'Income Detail' page by using one of the option listed above.

Note: For the purposes of this design, "Create" and "Edit" mode pages are defined as a page that allows the user to commit/save/update the information to the database by clicking the 'Save', Save and Return', or 'Save and Add Another' button.

2.1.4 Page Location

- **Global: N/A**
- **Local: N/A**
- **Task: N/A**

2.1.5 Security Updates

N/A

2.1.6 Page Mapping

N/A

2.1.7 Page Usage/Data Volume Impacts

N/A

3 REQUIREMENTS

3.1 Migration Requirements

DDID #	REQUIREMENT TEXT	Contractor Assumptions	How Requirement Met
2054	**Original:** The CONTRACTOR shall add a validation message on all pages when in "Edit" mode on the page and the user makes a change and tries to exit the page without saving. Assumption: This would not apply when the user hits the Cancel button. **Revised:** The CONTRACTOR shall add a validation message on all pages when in "Create" or "Edit" mode on the page and the user makes a change and tries to exit the page without saving. Assumption: This would not apply when the user hits the Cancel button.	It is assumed the validation message would occur when a user tries to leave a page from edit or create mode.	Notification message will display when user tries to navigate away from the page when changes were made to the page. This will only display for "Create" and "Edit" mode pages and they are navigating away from the page without saving the change or navigating by other means other than clicking the "Cancel" button.

CalSAWS

California Statewide Automated Welfare System

Design Document

CA-213988

ForgeRock – Replace Oracle IAM Security Stack

CalSAWS	DOCUMENT APPROVAL HISTORY	
	Prepared By	Raheem Raasikh
	Reviewed By	

DATE	DOCUMENT VERSION	REVISION DESCRIPTION	AUTHOR
02/13/2020	V1	Initial Design	Raheem
05/01/2020	V2	Updated User Flows	Sumeet
05/02/2020	V3	Updated the document formatting and added additional sections to align with the changes being made.	Matthew Lower
05/02/2020	V4	Update destination when logging into the system.	Matthew Lower
08/04/2020	V5	Exit button had incorrect navigation and further clarification on Inactive users.	Matthew Lower

Table of Contents

1 OVERVIEW

Purpose of this SCR is to replace the CalSAWS Oracle Security stack with the ForgeRock Security stack

1.1 Current Design

The authentication is handled using Oracle Identity and Access Management Products - Oracle Access Manager(OAM), Oracle Internet Directory(OID) and Oracle Virtual Directory (OVD). The OVD is configured to authenticate the user against County AD or CalSAWS AD or OID.

The Managed Personnel interface to OID functionality is currently handled by the LDAPHelper architecture component.

1.2 Requests

In November 2019, the Consortium engaged Accenture to modernize the IAM Security Stack supporting the CalSAWS (formerly LRS) application. The strategic direction from the Consortium is to leverage the ForgeRock Identity Platform to provide IAM Services to Consortium applications and users.

As part of this request the Oracle Security Stack used by application components will be replaced with ForgeRock Identity platform

Authentication:

Replace authentication for Audit and CalSAWS applications. For Audit replace current OAM Header authentication with FR OIDC provider authentication. For CalSAWS, add additional spring filter to support FR OIDC provider authentication for both regular staff users and collaborator users.

Authorization:

Pick up role information from DB instead of OID

Managed Personnel:

Replace current LDAP/OID methods in LDAPHelper with FR IDM/DS calls instead.

1.3 Overview of Recommendations

1. Update the display and functionality of the CalSAWS Login page to utilize the ForgeRock Security stack.
2. Update the Active Directory Search and Security Assignment page to facilitate user creation in the ForgeRock Security stack.
3. Update the CalSAWS application to use the ForgeRock Security stack. Adjust the following functionality to utilize ForgeRock in place of the Oracle Security stack:
    a. Login/Authentication

   b. Logout
   c. Session Timeout
   d. Active Directory Interface (LDAP)
   e. User Roles (Authorization)
4. Update the Audit application to use the ForgeRock Security stack. Adjust the following functionality to utilize ForgeRock in place of the Oracle Security stack:
   a. Login
   b. Logout
5. Update the LRS Web Services Accounts Endpoints to use the ForgeRock Security stack. Adjust the following functionality to utilize ForgeRock in place of the Oracle Security stack:
   a. Registered Users Authentication End Point
6. Update the OBIEE/BI Reports to use the ForgeRock Security stack. Adjust the following functionality to utilize ForgeRock in place of the Oracle Security stack:
   a. Single Sign On
   b. User Roles
7. Update the User Flows to account for the ForgeRock Security stack. Adjust the following User Flows to utilize ForgeRock in place of the Oracle Security stack:
   a. Creating user with AD LInked identity
   b. Creating user with Non AD linked identity
   c. Removing CalSAWS user
   d. Revoking a user
   e. Re-enabling a user
   f. Change Non AD linked user password
   g. User Login Flow

1.4 Assumptions

1. Users having "*lacounty.gov" or “*lasd.org” or “*lacera.org” email addresses should ALWAYS get authenticated to LA ISD AD.
2. ALL users that should be authenticated against LA ISD AD have "*lacounty.gov" or “*lasd.org” or “*lacera.org” email addresses.
3. Users having "*calsaws.org" or “*calaces.org” email addresses should ALWAYS get authenticated to CalSAWS AD.
4. ALL users that should be authenticated against CalSAWS AD have "*calsaws.org" or “*calaces.org" email addresses.
5. A one time bulk user load import will be done into ForgeRock with email address populated for AD linked identities from AD mail attribute. This will occur with CA-212922.

2 RECOMMENDATIONS

2.1 CalSAWS Login Page

2.1.1 Overview

With the introduction of the ForgeRock Security Stack, the backend functionality for Authentication is being altered. In addition, the LRS/CalSAWS Login page is being adjusted to meet the requirements of the applications supported in the CalSAWS.net domain. The functionality for the end user will remain the same, however the visual aspects of the page are being altered to utilize modern design concepts.

2.1.2 CalSAWS Login Page

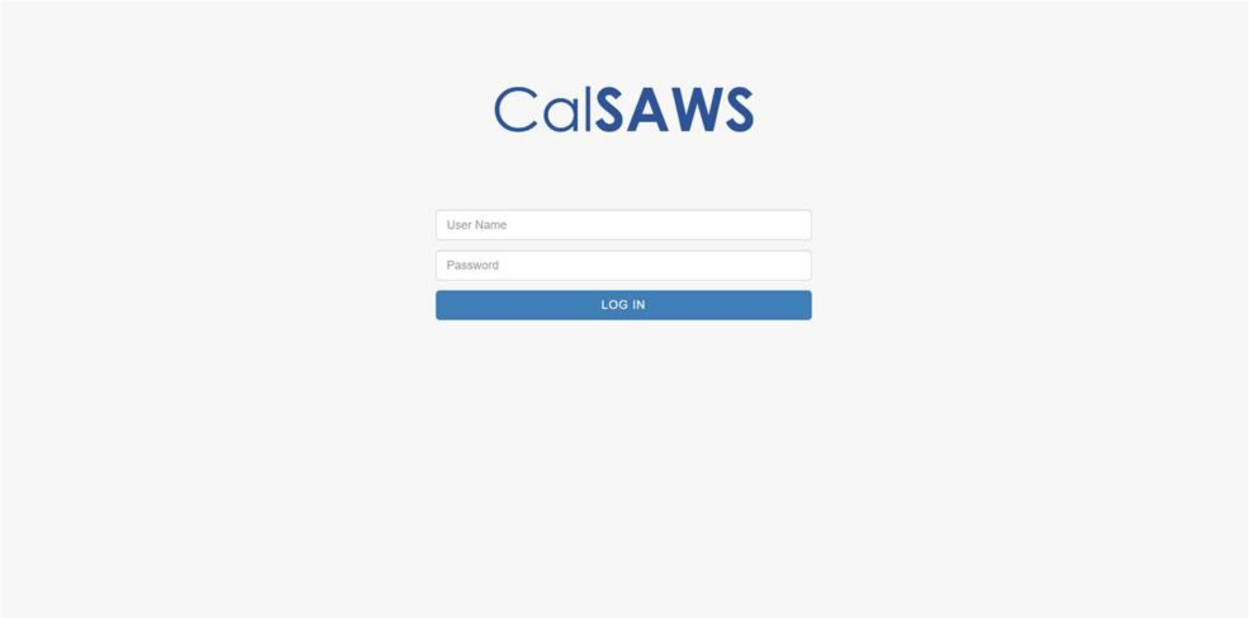
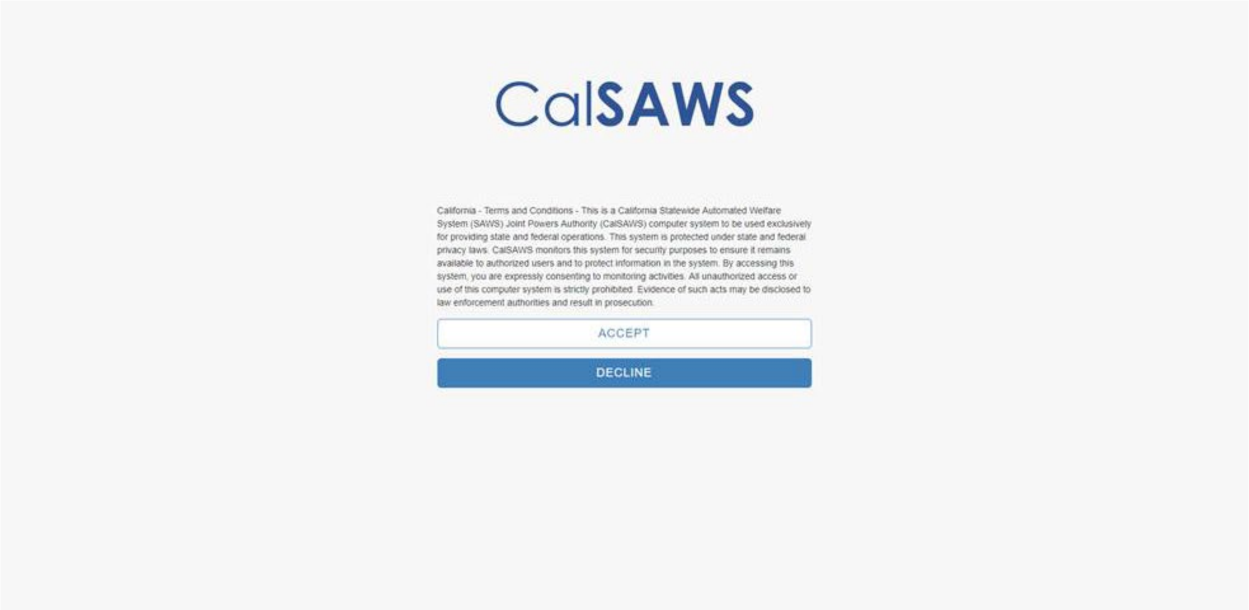
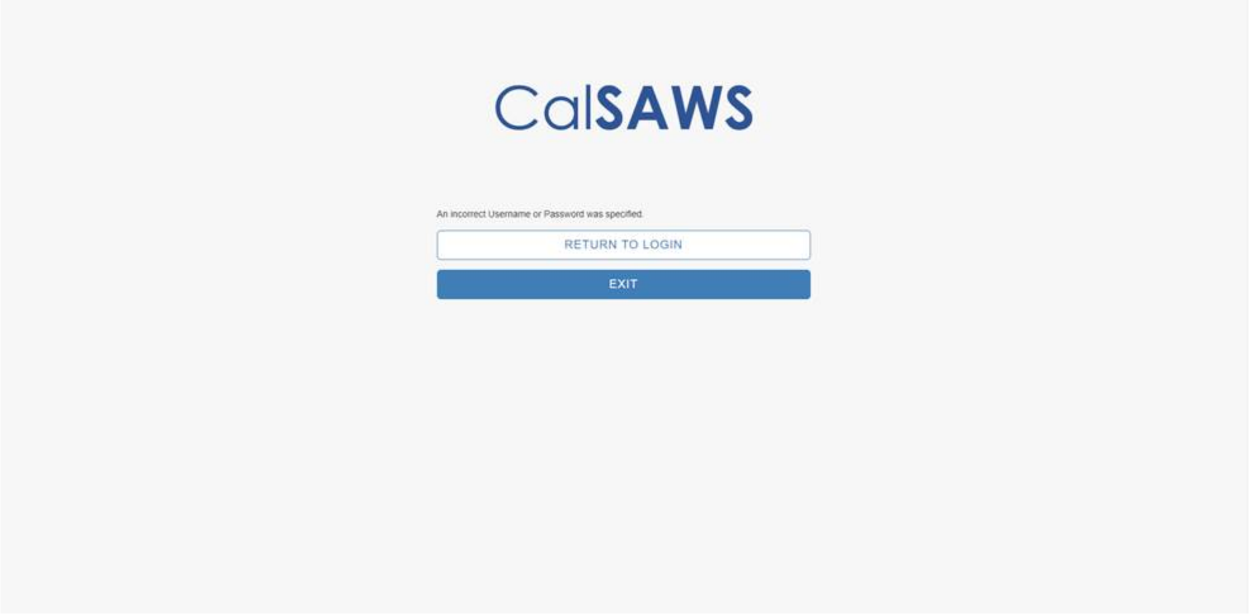


Figure 2.1.1 – CalSAWS Login Page



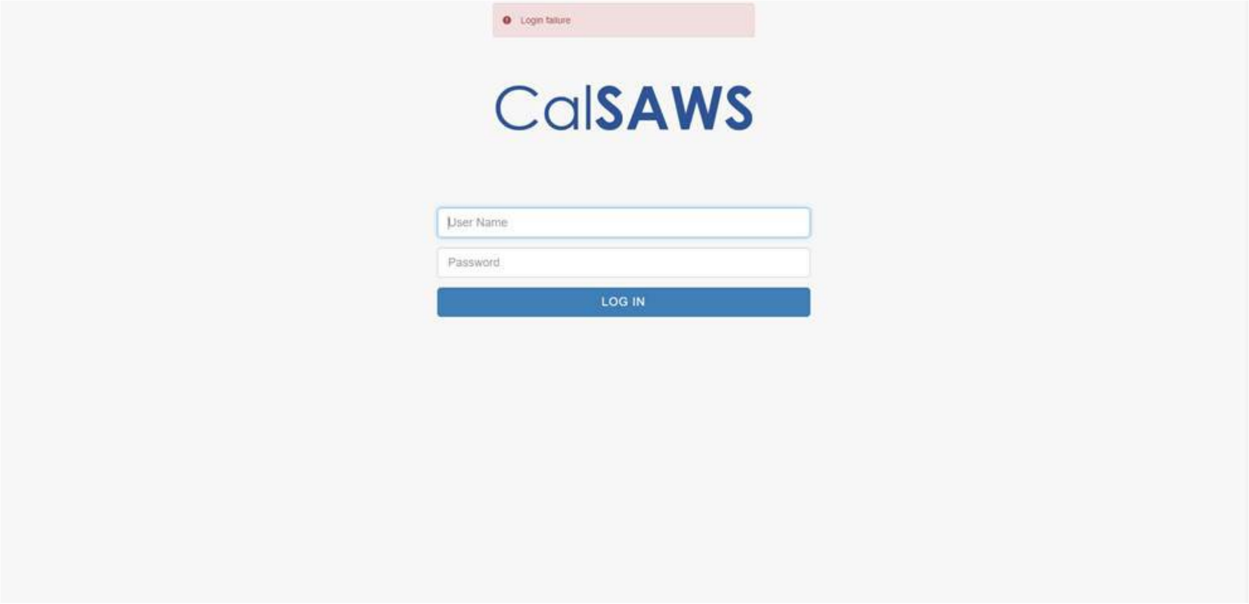
California - Terms and Conditions - This is a California Statewide Automated Welfare System (SAWS) Joint Powers Authority (CalSAWS) computer system to be used exclusively for providing state and federal operations. This system is protected under state and federal privacy laws. CalSAWS monitors this system for security purposes to ensure it remains available to authorized users and to protect information in the system. By accessing this system, you are expressly consenting to monitoring activities. All unauthorized access or use of this computer system is strictly prohibited. Evidence of such acts may be disclosed to law enforcement authorities and result in prosecution.

Figure 2.1.2 – CalSAWS Login Page – Terms and Conditions



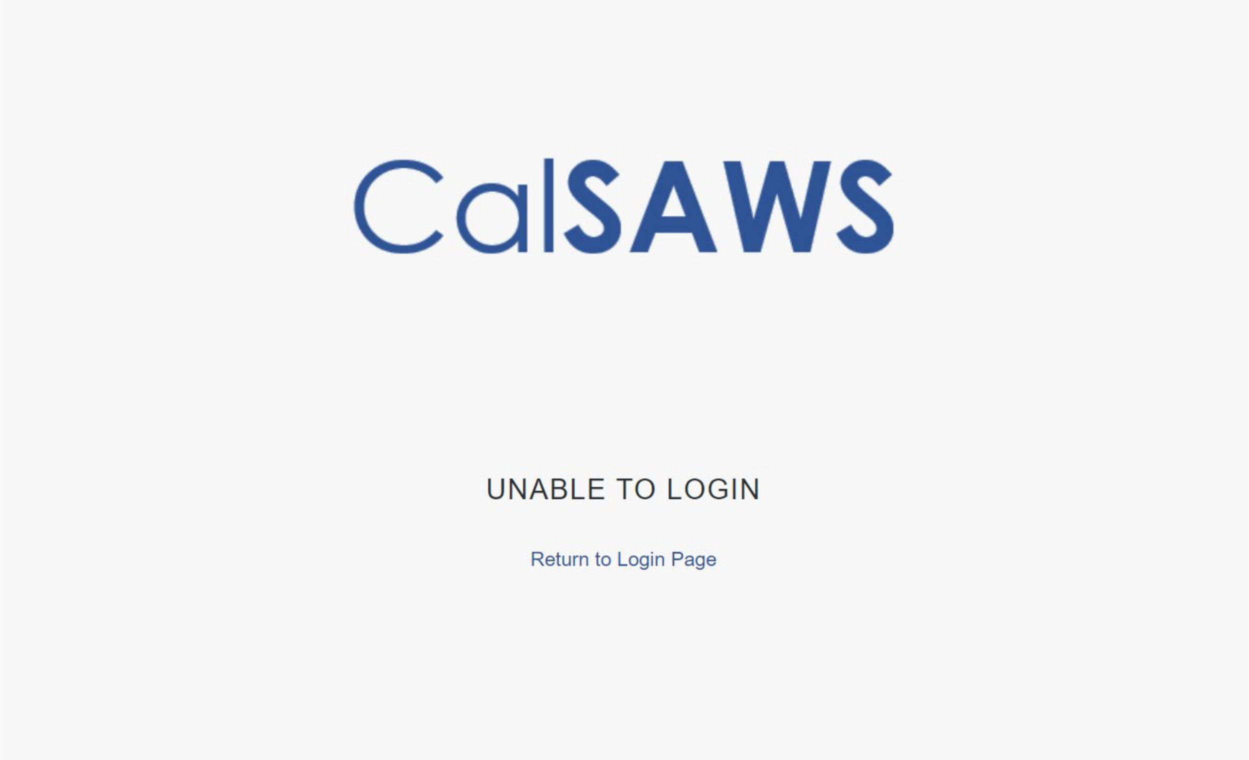
An incorrect Username or Password was specified.

Figure 2.1.3 – CalSAWS Login Page – Incorrect User Name/Password



Login failure

Figure 2.1.5 – CalSAWS Login Page – Other Error Message



UNABLE TO LOGIN

Figure 2.1.6 – CalSAWS Unable to Login Page

2.1.3 Description of Changes

1. CalSAWS Logo – This is the logo used for the domain and will display at the top of the screen.
2. User Name – This field will capture the user name that the user is using to sign into the application with.

Note: The Employee Number will be utilized for this field.

3. Password – This field will be used by the user to enter their password which will be used to authenticate the user and grant access to the application. When entering characters into this field, they will be masked to hide the value for security purposes.
4. Log In – This button will navigate the user to the Terms and Conditions page with the information they entered stored until they Accept the terms and conditions.
5. Terms and Conditions – The Terms and Conditions is used to notify the user of what is agreed to when using the CalSAWS system.
    a. Accept – This button will signify that the user agrees to what is stated in the terms and conditions. The user would then be authenticated and navigated to the Homepage. If they Accept the terms and conditions but cannot be authenticated, a message will display alerting the user as to why they could not complete the Log In process.
    b. Decline – This button will close the Terms and Conditions and will not proceed with attempting to grant access to the application. The information entered on the Log In page will be cleared out.

    Note: SCR CA-207490 updated the verbiage of the Terms and Conditions to the following which will is being utilized by the CalSAWS Login page:

    > "California - Terms and Conditions
    > This is a California Statewide Automated Welfare System (SAWS) Joint Powers Authority (CalSAWS) computer system to be used exclusively for providing state and federal operations. This system is protected under state and federal privacy laws. CalSAWS monitors this system for security purposes to ensure it remains available to authorized users and to protect information in the system. By accessing this system, you are expressly consenting to monitoring activities. All unauthorized access or use of this computer system is strictly prohibited. Evidence of such acts may be disclosed to law enforcement authorities and result in prosecution."
6. If the user could not complete the log in process due to a validation message, they will be brought to a page with the following buttons.
    a. Return to Login – This button will navigate the user back to the Log In page with the values previously entered cleared out.
    b. Exit – This button will navigate the user to either the Unable to Login page or the Login Page. If the user had already navigated to the Unable to Login page then the user will be navigated to the Login page. On the Unable to Login page there will be a link called Return to Login Page which will return the user to the Log In page.

2.1.4 Page Location

This page is navigated to whenever the system needs to authenticate the user. There is no change to when this page will be displayed.

2.1.5 Page Validation

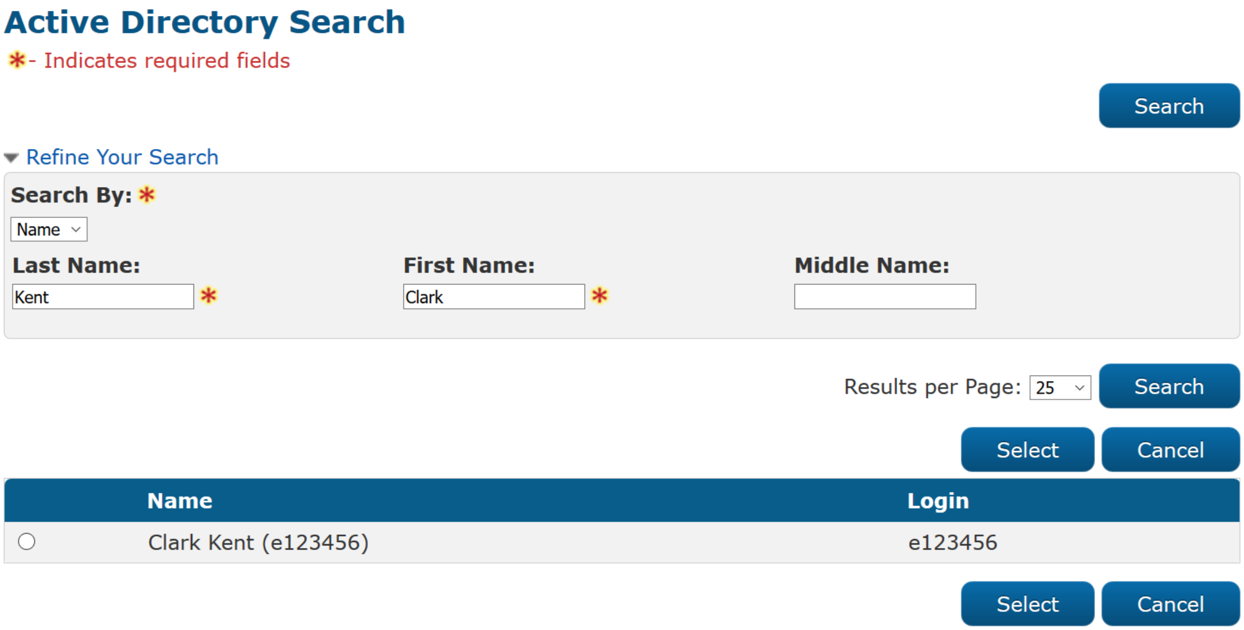
1. An incorrect Username or Password was specified.
    a. Triggered when the user attempts to Log in with the incorrect Credentials or an inactive account.
2. Your CalSAWS AD account is locked out or has expired. Please contact the CalSAWS IT Helpdesk.
    a. Triggered when the user's account is locked out for a CalSAWS AD account.
3. Your County AD account is locked out or has expired. Please contact your County IT Helpdesk
    a. Triggered when the user's account is locked out for an AD account.
4. Your ForgeRock account is locked out or has expired. Please contact the CalSAWS IT Helpdesk.
    a. Triggered when the user's account is locked out for a ForgeRock Internal account.
5. An error message will appear at the top of the Login page if there are any additional errors that are triggered and not accounted for in the above criteria.

2.2 Active Directory Search

2.2.1 Overview

The Active Directory Search page retrieves accounts that were created in the Active Directory. This page is navigated to from the Security Assignment page when creating a User Name for the application or from the Resource Detail page. The changes to this page are not viewable to the user.

2.2.2 Active Directory Search Page



Active Directory Search

*- Indicates required fields

Search By: * Name

Last Name: Kent *

First Name: Clark *

Middle Name:

Results per Page: 25

	Name	Login
○	Clark Kent (e123456)	e123456

Figure 2.1.1 – CalSAWS Login Page

2.2.3 Description of Changes

1. Upon retrieving the user accounts, also retrieve the account's E-mail address to be used for ForgeRock account creation when saving the Security Assignment Detail page. The E-mail address will not be displayed to the user.

2.2.4 Page Location

- **Global: Admin Tools**
- **Local: Office Admin**
- **Task: Staff**

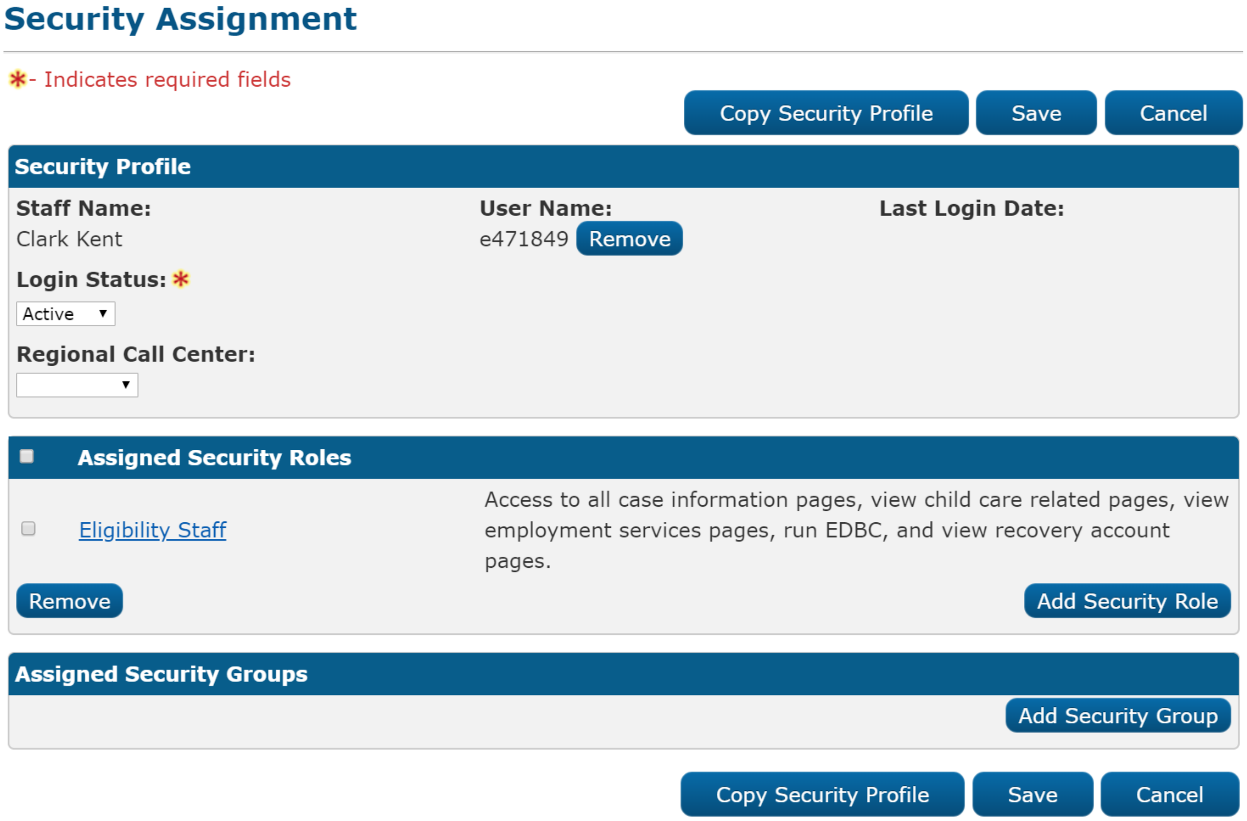
- **Global: Resource Databank**
- **Local: Resources**
- **Task: Resource Detail**

2.3 Security Assignment

2.3.1 Overview

The Security Assignment page is used to assign security to Staff records in order to facilite the system needs of the worker. The changes to this page are not viewable to the user.

2.3.2 Security Assignment Page



Security Assignment

*- Indicates required fields

Security Profile

Staff Name: Clark Kent

User Name: e471849

Last Login Date:

Login Status: * Active

Regional Call Center:

Assigned Security Roles

□	Eligibility Staff	Access to all case information pages, view child care related pages, view employment services pages, run EDBC, and view recovery account pages.

Assigned Security Groups

Figure 2.1.1 – Security Assignment Page

2.3.3 Description of Changes

1. Upon navigating to this page from the Active Directory Search page, send the email address that is associated to the Active Directory record to ForgeRock for user user managment purposes. The E-mail address will not be displayed to the user.

2.3.4 Page Location

- **Global: Admin Tools**

- **Local: Office Admin**
- **Task: Staff**

2.4 LDAPHelper Role Information

2.4.1 Overview

Currently there are pages that access OID to get or pass Security Role information. As ForgeRock will not be storing security roles at this time, the functionality to get these roles will be removed from LDAPHelper.

2.4.2 Description of Changes

1. Remove the calls to LDAPHelper which gets or sets role information in OID from the following pages:
    a. Oversight Agency Staff Detail
    b. Security Assignment
    c. County Security Role List
    d. County Security Role Detail

    Note: These changes are not viewable by the user.

2.5 CalSAWS Application

2.5.1 Overview

The implementation of ForgeRock with the current CalSAWS application requires updates made to the way the application interacts with the Authentication and Authorization framework.

2.5.2 Description of Changes

1. Login/Authentication:
    a. Use Spring Security to intercept users' requests and check if they have valid access tokens generated from ForgeRock. This replaces the functionality provided currently by Oracle's Webgate plugin running within the Oracle HTTP Server, both of which will be replaced.
    b. When user navigates to the CalSAWS application url and if they are not already logged in, they will be redirected to a login page for authentication. If they have a valid access token having successfully logged in earlier they will be presented with their requested page

c. User will be presented with a CalSAWS login page generated by ForgeRock. This new login page will continue to support features for recording user transactions in AMP application.
d. Once logged in, UserProfile with rights will be generated so that user can access pages they have rights to.
e. To lower the risk of impact to the entire application due to potential issues of slower responses from ForgeRock or related infrastructure, control the thread pool allocated to the login components. This is a pattern commonly used in CalSAWS application when interacting with external components.

2. Logout:
   When the user clicks the logout link, their Weblogic and ForgeRock CalSAWS sessions will be terminated thus requiring users to login to CalSAWS again when they visit again. If the user has other active sessions like Audit and OCAT, then those sessions will remain alive and user will continue to work in those applications.

3. Session Timeout:

   When the user's session is timed out due to inactivity after 20 minutes, their ForgeRock session will be terminated causing them to have to login again when they are ready to continue.

4. Active Directory Interface (LDAP):

   The Architecture package will be updated to use the ForgeRock REST APIs to provide an interface with ForgeRock for the application functionality. The LDAPHelper methods will be updated to use the ForgeRock REST APIs. The list of methods to be changed is added in the attached document - ForgeRock_Tech_Impact.xlsx. These REST API's will interact with ForgeRock components like Identity Gateway, Identity Management, Access Management and Directory Services to access the CalSAWS Active Directory, and LA County ISD Active Directory.

5. User Roles (Authorization):

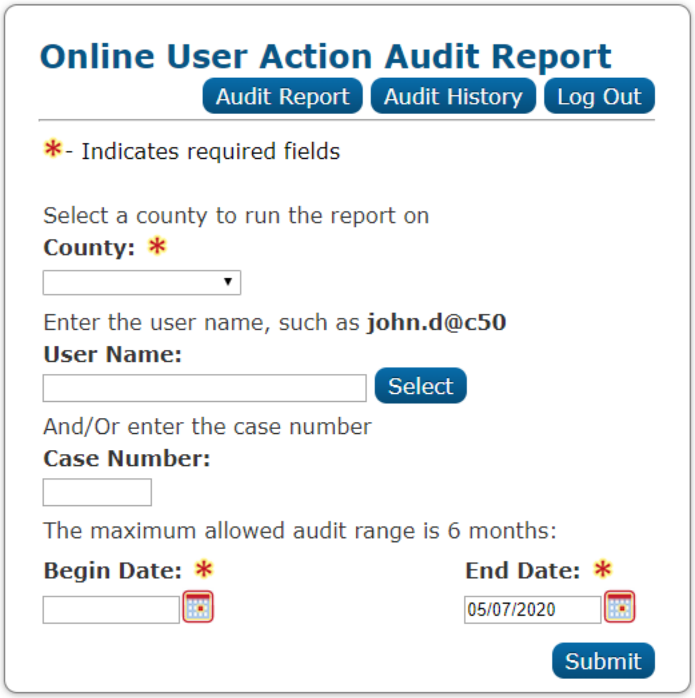
   Currently user roles are stored in the CalSAWS database as well as the Oracle Internet Directory (OID) and referenced from both sources. This SCR will change the roles to be stored only in the database and provide better data integrity. Refer to the Online Impact Analysis attachment document for the pages that are impacted by this change.

2.6 Audit Application

2.6.1 Overview

The implementation of ForgeRock with the current Audit application requires updates made to the way the application interacts with the Authentication and Authorization framework.

2.6.2 Online User Action Audit Report Page



Online User Action Audit Report

*- Indicates required fields

Select a county to run the report on

County: *

Enter the user name, such as **john.d@c50**

User Name:

And/Or enter the case number

Case Number:

The maximum allowed audit range is 6 months:

Begin Date: *

End Date: * 05/07/2020

Figure 2.1.1 – Online User Action Audit Report Page

2.6.3 Description of Changes

1. Login/Authentication:
   a. Update the Audit application to forward unauthenticated users through Spring Security to the CalSAWS login page and after they successfully login they will be forwarded back to the Audit homepage if they have an Auditor role. This will create a ForgeRock session and an application session for that user and a valid access token will be returned by ForgeRock.
   b. When users logged in the CalSAWS application access the Audit link in the Admin Tools global navigation and Admin local navigation tab they will be forwarded to the Audit homepage.
2. Logout:
   a. Create a logout icon with hyperlink on the Audit homepage similar to the CalSAWS application logout. Clicking on this link

will terminate the user's Audit application and ForgeRock sessions. If the user logs out of the Audit Application and they have a CalSAWS application session alive, that session will still continue until they explicitly log out of CalSAWS.

2.7 LRS Web Services Accounts Endpoint

2.7.1 Overview

The implementation of ForgeRock with the current LRS Web Services requires updates made to the way the Web Services interacts with the Authentication and Authorization framework.

2.7.2 Description of Changes

1. The internal mobile apps uses this endpoint to authenticate CalSAWS registered users who use the internal check-in mobile app. The Architecture method will be updated to authenticate this endpoint users against ForgeRock.

2.8 OBIEE/BI Reports

2.8.1 Overview

The implementation of ForgeRock with the current OBIEE/BI Reports requires updates made to the way the reports interacts with the Authentication and Authorization framework.

2.8.2 Description of Changes

1. Single Sign On:
    a. OBIEE will be configured to authenticate user against ForgeRock using SAML (Security Assertion Markup Language).
2. User Roles:
    a. OBIEE will be re-configured to read user roles from CalSAWS database.

2.9 User Flows

2.9.1 Overview

The user flows are being altered to function with ForgeRock. The user Creation flow and other flows can be found in the attached 'CalSAWS User Flows – ForgeRock.pdf' document.

2.9.2 Description of Changes

1. Creating user with AD linked identity (Flow 1 in Document):
    a. CalSAWS-created AD-linked identities will be created with the Email address of the User's AD account, regardless of what email is assigned in the staff record. AD-linked identities refer to LA County ISD AD and CalSAWS.org AD. Primary email address from the Staff Detail page is not used for the creation of these identities.
    b. Any update to the email address in CalSAWS Application will not flow into ForgeRock.
    c. If the user does not have an email address in Active Directory, the following dummy email address will be added in ForgeRock for that user –
        i. County AD linked user without email address – <username>@default.lacounty.gov
        ii. CalSAWS AD linked user without email address - <username>@default.calsaws.org
    d. Prior to user creation in ForgeRock, the user will be searched with email address and if found the AD User name will be populated for that user, instead of creating a new user in ForgeRock.
    e. Email addresses will be unique in ForgeRock for AD linked identities.
    f. There will be only one active unique username in ForgeRock at any time.
2. Creating user with Non AD linked identity (Flow 2 in Document):
    a. CalSAWS-created Non-AD (internal) identities will be created with NO Email address. It will be left blank.
3. Removing CalSAWS User (Flow 3 in Document):
    a. For removing a CalSAWS user, the user name will be blanked out for that user in ForgeRock.
4. Revoking a user (Flow 4 in Document):
    a. For revoking a user, the accountStatus attribute will be set to 'inactive' in in ForgeRock. User with inactive status will not be able to login into CalSAWS application.
5. Re-enabling a user (Flow 5 in Document):
    a. A user will be re-enabed by setting the accountStatus attribute in ForgeRock to 'active'.

6. Change Non AD linked User Password (Flow 6 in Document)
7. User Login flow (Flow 7 in Document):
   a. When User logs in, only active user identities will be authenticated against. The active user is determined by ForgeRock custom attribute ‘accountStatus’ value of ‘active’

2.10 Tech Changes

2.10.1 Overview

With the implemtation of ForgeRock, additional changes are necessary to ensure the functionality the user are use to remains the same. Below list the additional area that need to be addressed to persist the user experience. These changes will not be viewable to the user.

2.10.2 Description of Changes

1. URL Protection:
   a. Protected resources within CalSAWS will continue to be protected with Spring Security instead of Oracle Access Manager.
2. Custom Attributes:
   a. Custom Attributes will be added in ForgeRock to support functionalities previously provided by OID. These are listed in the ‘ForgeRock_Tech_Impact.xlsx’ document [Attributes worksheet].

3 SUPPORTING DOCUMENTS

Number	Functional Area	Description	Attachment
1.	Tech Arch	CalSAWS User Flows	PDF CalSAWS User Flows - ForgeRock.pdf

4 REQUIREMENTS

4.1 Project Requirements

REQ #	REQUIREMENT TEXT	How Requirement Met
3.4.1.3.2	The LRS shall ensure that a change made to a specific Users access, or denial of access, is updated to the LRS in real-time mode, so that the User(upon next attempt to relogin) may have immediate access, or immediate denial of access, to the LRS or a function within the LRS.	User access will not be affected by the introduction of the new authentication framework
2.1.2.5	The LRS shall prominently display confidentiality statements and privacy protections upon login.	The terms and conditions will display before a user can access the application content.

5 MIGRATION IMPACTS

[Document any migration impacts such as data model or potential business process changes]

SCR Number	Functional Area	Description	Impact	Priority	Address Prior to Migration?

6 OUTREACH

[Include any specific outreach that needs to occur with implementation i.e. a CIT, a special webcast or onsite demonstration, any lists, etc…]

7 APPENDIX

[Include any supplementary items that my not fit in the Description section. Examples could include flow charts, lengthy code tables, etc.…]