

CalSAWS

California Statewide Automated Welfare System

Design Document

CA-203636 | DDID 1967

Medi-Cal Renewal Periods for MSP Households

CalSAWS	DOCUMENT APPROVAL HISTORY	
	Prepared By	Renee Gustafson
	Reviewed By	Amy Gill

DATE	DOCUMENT VERSION	REVISION DESCRIPTION	AUTHOR
11/21/2019	1.0	Original Draft	Renee Gustafson
12/09/2019	1.1	Added Data Change criteria and journal. Updated EDBC rules. Added Supporting documents	Renee Gustafson
12/18/2019	1.2	Updated criteria for one-time data change to populate existing MC programs without an appropriate Redetermination record.	Renee Gustafson
03/23/2020	1.3	Content Revision: Updated criteria from July to September and updated following roll-out dates in yellow	Tisha Mutreja

Table of Contents

1	Overview	4
	1.1 Current Design.....	4
	1.2 Requests.....	5
	1.3 Overview of Recommendations.....	5
	1.4 Assumptions	5
2	Recommendations.....	6
	2.1 Medi-Cal Rules Updates	6
	2.1.1 Overview	6
	2.1.2 Description of Changes	6
	2.1.3 Programs Impacted	6
	2.1.4 Performance Impacts	6
	2.2 Data Change	7
	2.2.1 Overview	7
	2.2.2 Description of Change.....	7
	2.2.3 Estimated Number of Records Impacted/Performance.....	7
	2.3 Automatic Journal Entry	8
	2.3.1 Overview	8
	2.3.2 Description of Change.....	8
	2.3.3 Programs Impacted	8
	2.3.4 Performance Impacts	8
3	Requirements.....	9
	3.1 Migration Requirements.....	9

1 OVERVIEW

Per All County Welfare Directors Letter (ACWDL) 08-21, 22 California Code of Regulations (CCR) § 50141, § 50189, Welfare and Institutions Code (WIC) 14005.37 and the Medi-Cal Eligibility Procedures Manual (MEPM), Qualified Medicare Beneficiaries (QMB) are subject to an annual redetermination. CalSAWS Medi-Cal EDBC rules will now set a redetermination period for QMB with Supplemental Security Income/State Supplementary Payment (SSI/SSP). A one-time data change will establish a redetermination period for any active Medi-Cal program in CalSAWS without an appropriate redetermination period.

1.1 Current Design

In CalSAWS, the Medi-Cal EDBC rules do not set a redetermination period for Medi-Cal programs where all individuals are eligible for QMB and have SSI/SSP. CalSAWS determines the redetermination period for QMB without SSI/SSP as follows:

Intake

Redetermination Begin Date: First day of the month of the Beginning Date of Aid (BDA)

RE Due Date: Last day of the month of 'Begin Date + 11 months'

RE

Redetermination Begin Date: First day of the month of the EDBC Benefit Month

RE Due Date: EDBC Last day of the month of 'Begin Date + 11 months'

In C-IV, the Medi-Cal EDBC rules set a redetermination period for all active Medi-Cal programs.

C-IV uses the same criteria as stated above to determine the redetermination periods for QMB with or without SSI/SSP.

1.2 Requests

ACWDL 08-21 clarifies that Medicare Savings Programs (MSP) are Medi-Cal programs and requires MSP eligibility determinations, including redeterminations, for all Medicare eligible Medi-Cal applicants and beneficiaries; this includes SSI Medi-Cal beneficiaries.

With that in mind, the application and redetermination requirements of 22 CCR § 50141, § 50189, and WIC 14005.37 apply. Individuals on QMB with SSI/SSP need to be redetermined for QMB eligibility annually.

Lastly, the MEPM Q&A regarding individuals on QMB with SSI/SSP found on page 5L-30, question 6, provides a direct answer to the question about redeterminations for this population.

6. Is a QMB redetermination required for SSI recipients?

Answer: Yes. They are considered aged, blind, or disabled and should be evaluated yearly.

When a Medi-Cal program has all individuals eligible for QMB and all have SSI/SSP, the individuals are not required to turn in a Renewal Packet, but the worker will perform an annual ex parte review and perform a redetermination.

1. Update CalSAWS Medi-Cal EDBC rules to set a redetermination period for QMB with SSI/SSP.
2. Add a redetermination record for existing Medi-Cal programs without an appropriate redetermination record and create a journal.

1.3 Overview of Recommendations

1. Update Medi-Cal EDBC rules to establish a redetermination period for QMB with SSI/SSP.
2. Perform a one-time data change to establish a redetermination record for all Medi-Cal programs without an appropriate redetermination record.
3. Create a journal entry for cases updated by the one-time data change.

1.4 Assumptions

1. CalSAWS will not generate an annual Renewal packet for Medi-Cal Programs where all individuals are QMB with SSI/SSP.
2. The one-time data change will establish redetermination periods with a Due Date in the future for all existing Medi-Cal programs that do not have an appropriate redetermination period. The one-time data change will not update the redetermination period for any active Medi-Cal programs with an overdue RE.

2 RECOMMENDATIONS

2.1 Medi-Cal Rules Updates

2.1.1 Overview

Update Medi-Cal EDBC rules to establish a redetermination period for QMB with SSI/SSP.

2.1.2 Description of Changes

1. Update Medi-Cal EDBC rules to establish a redetermination period when all individuals are active for QMB with SSI/SSP. Establish the redetermination period using the same redetermination logic as QMB without SSI/SSP; this applies to new applications and Medi-Cal EDBCs run with "RE" Run Reason.

2.1.3 Programs Impacted

Medi-Cal

2.1.4 Performance Impacts

No change.

2.2 Data Change

2.2.1 Overview

Perform a one-time data change to establish a redetermination record for all Medi-Cal programs without an appropriate redetermination record.

2.2.2 Description of Change

1. Identify active Medi-Cal programs with the following criteria:
 - a. There is at least one active individual on the Medi-Cal program effective on or after May 2020 benefit month.
 - b. A redetermination record does not exist for the Medi-Cal program.Or
The latest redetermination record for the Medi-Cal program is completed and a new redetermination record for the Medi-Cal program does not exist.
2. Create a new redetermination record for each identified Medi-Cal program with the following values:
 - a. If the BDA is on or after **September** 2019, then
Begin Date: First day of the month of BDA
Due Date: Last day of the month for 'Begin Date + 11 months'

Example

BDA	Begin Date	Due Date
September 2019	September 01, 2019	August 31, 2020
January 2020	January 01, 2020	December 31, 2020

- b. If the BDA is prior to **September** 2019, then
Begin Date: First day of the month of BDA with year 2020
Due Date: Last day of the month for 'Begin Date + 11 months'

BDA	Begin Date	Due Date
August 2019	August 01, 2020	July 31, 2021
January 2018	January 01, 2020	December 31, 2020

2.2.3 Estimated Number of Records Impacted/Performance

The one-time data change will update approximately 32,000 Active Medi-Cal programs without an appropriate redetermination record.

2.3 Automatic Journal Entry

2.3.1 Overview

Create a journal entry for cases updated by the one-time data change.

2.3.2 Description of Change

1. Create one Journal Entry per case with the following values for cases updated by the one-time data change:

Journal Category: All

Journal Type: Basic Information

Short Description: MC RE Due Date updated

Long Description: The system established a redetermination record for the Medi-Cal program due to a one-time data change for Medi-Cal programs without an appropriate redetermination record.

2.3.3 Programs Impacted

Medi-Cal

2.3.4 Performance Impacts

N/A

3 REQUIREMENTS

3.1 Migration Requirements

DDID #	REQUIREMENT TEXT	Contractor Assumptions	How Requirement Met
1967	<p>As Side-by-Side sessions were focused on comparing the front end (online pages) functionality of the application, the CONTRACTOR shall budget an allowance of twenty-nine thousand, one hundred fifty-five hours (29,155) to accommodate for any Unforeseen differences in the code base that result in additional requirements.</p> <p>The requirements for the allowance of hours must be finalized and approved by the CONSORTIUM for the CONTRACTOR to meet design, build and System Test milestones, subject to the requirements meeting requirements in the LRS Agreement.</p> <p>As the requirements for the designated SCRs are identified, the SCRs will be calculated by the CONTRACTOR and reviewed and prioritized by the CONSORTIUM for approval through the County Change Control Board process.</p>	<ul style="list-style-type: none"> Estimates will include the necessary Tasks in the software development lifecycle required to implement the CalSAWS DD&I SCR including deployment and change management. For the new requirements to be included with CalSAWS DD&I UAT preparation activities (targeted to begin April 2021 for C-IV), the requirements for the unforeseen Differences allowance hours must be finalized, approved by the CONSORTIUM and added to the CalSAWS DD&I SOR by July 1, 2020 for the CONTRACTOR to meet design, build and System Test milestones. 	<p>The System will now determine the effective start and end date of the Redetermination period for MSP individuals on QMB with SSI/SSP.</p>

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

Table of Contents

1	Overview	5
1.1	Current Design.....	5
1.2	Requests.....	5
1.3	Overview of Recommendations.....	5
1.4	Assumptions	6
2	Recommendations.....	7
2.1	CalSAWS Login Page	7
2.1.1	Overview	7
2.1.2	CalSAWS Login Page.....	7
2.1.3	Description of Changes	9
2.1.4	Page Location	10
2.1.5	Page Validation.....	10
2.2	Active Directory Search.....	11
2.2.1	Overview	11
2.2.2	Active Directory Search Page.....	11
2.2.3	Description of Changes	11
2.2.4	Page Location	11
2.3	Security Assignment	12
2.3.1	Overview	12
2.3.2	Security Assignment Page.....	12
2.3.3	Description of Changes	13
2.3.4	Page Location	13
2.4	LDAPHelper Role Information	13
2.4.1	Overview	13
2.4.2	Description of Changes	13
2.5	CalSAWS Application.....	13
2.5.1	Overview	13
2.5.2	Description of Changes	13
2.6	Audit Application	15
2.6.1	Overview	15
2.6.2	Online User Action Audit Report Page.....	15
2.6.3	Description of Changes	15

2.7	LRS Web Services Accounts Endpoint	16
2.7.1	Overview	16
2.7.2	Description of Changes	16
2.8	OBIEE/BI Reports	16
2.8.1	Overview	16
2.8.2	Description of Changes	16
2.9	User Flows	17
2.9.1	Overview	17
2.9.2	Description of Changes	17
2.10	Tech Changes	18
2.10.1	Overview	18
2.10.2	Description of Changes	18
3	Supporting Documents	18
4	Requirements	19
4.1	Project Requirements	19
5	Migration Impacts	20
6	Outreach	21
7	Appendix	21

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

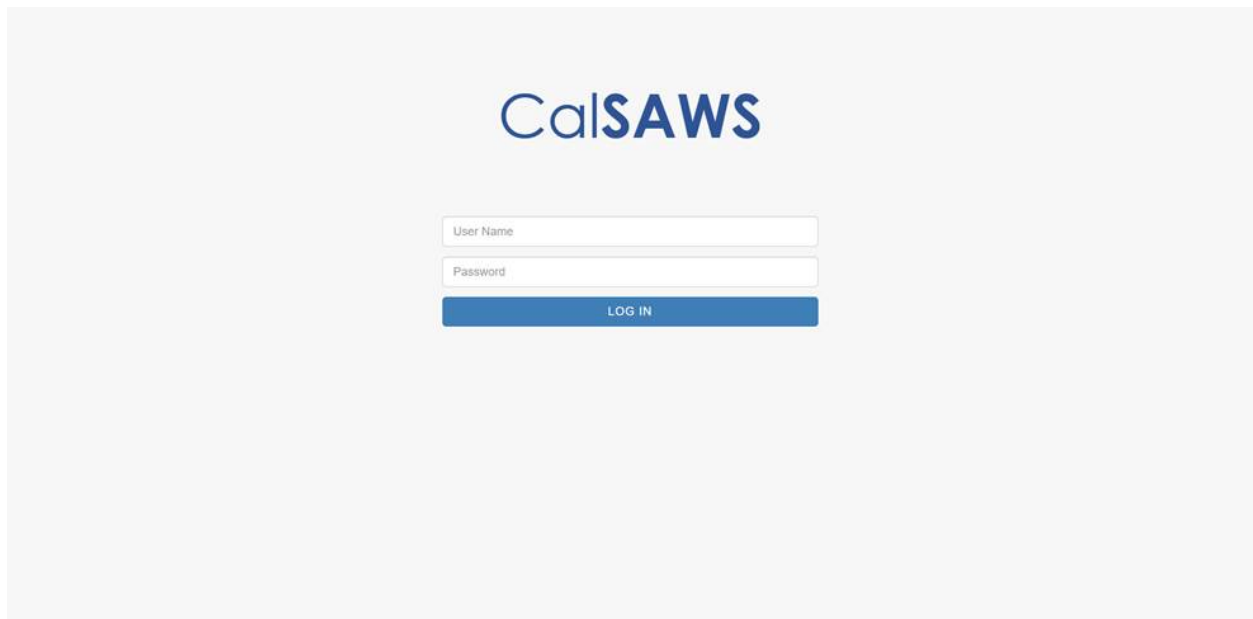


Figure 2.1.1 – CalSAWS Login Page

CalSAWS

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.

ACCEPT

DECLINE

Figure 2.1.2 – CalSAWS Login Page – Terms and Conditions

CalSAWS

An incorrect Username or Password was specified.

RETURN TO LOGIN

EXIT

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

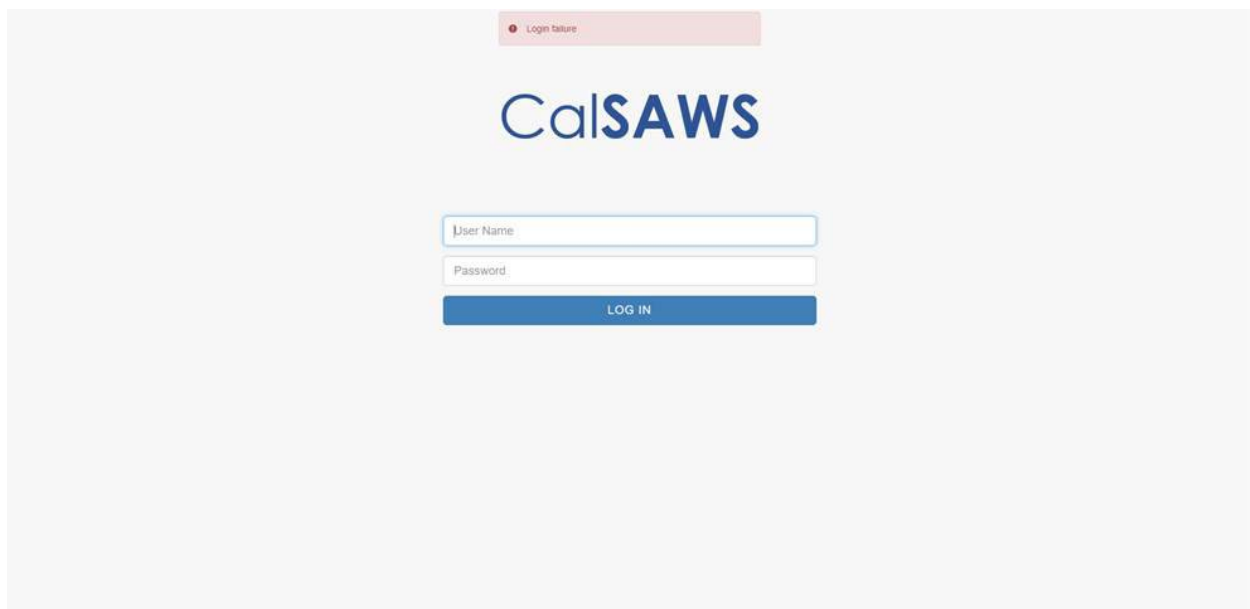


Figure 2.1.5 – CalSAWS Login Page – Other Error Message

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 page they were trying to access as long as they have the proper system security rights for the destination page. 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 the Unable to Login page. Which will have a link called Return to Login Page which will return the user tot 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.
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.

- 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

▼ Refine Your Search

Search By: *

Name

Last Name: *

First Name: *

Middle Name:

Results per Page:

	Name	Login
<input type="radio"/>	Clark Kent (e123456)	e123456

Figure 2.1.1 – CalSAWS Login Page

2.2.3 Description of Changes

- 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 facilitate 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

Copy Security Profile Save Cancel

Security Profile

Staff Name: Clark Kent	User Name: e471849 Remove	Last Login Date:
Login Status: * Active ▾		
Regional Call Center: ▾		

Assigned Security Roles

<input type="checkbox"/>	Eligibility Staff	Access to all case information pages, view child care related pages, view employment services pages, run EDBC, and view recovery account pages.
Remove		Add Security Role

Assigned Security Groups

Add Security Group

Copy Security Profile Save Cancel

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 management 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

Audit Report Audit History Log Out

* - 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

Submit

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-enabled 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 implementation 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	 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 may not fit in the Description section. Examples could include flow charts, lengthy code tables, etc....]