DSD - Section 6

D-4.2-03 – IHSS CMIPS Detailed System Design (DSD) (R2025.03.01) Section 6

Version 1.0

03/28/2025

Table of Contents

DSD 6/Architecture – System Security

DSD 6/Architecture – System Security/System Security Topic Area

There are four main applications interacting to provide the overall security for CMIPS. They are:

- Web Portal authentication and authorization via LDAP, which is also used for application-to-application, ServiceNow, WAS Middleware Administration, DB2 Middleware Administration, and AIX-LPAR Administration
- Cúram authorization to screens, location, units, business processes, data, work queues and links
- BusinessObjects to reports and report data
- Advantage to payroll data

The User ID when created for Web Portal, Case Management (Cúram), and Reporting (Business Objects) is assigned a location code of:

- County for Web Portal and Reporting (Business Objects)
- County and District Office for Case Management (Cúram)

Note:
For all statewide entities a county code of 99 is assigned to represent statewide visibility

1. IHO (WPCS) is are assigned a county code of 99 for statewide visibility but BusinessObjects and Cúram security role designate them as IHO personnel

DSD 6/Architecture – System Security/System Security Topic Area/CMIPS Web Portal

The Web Portal houses the entire authentication of a user via a single sign-on to all aspects of CMIPS.

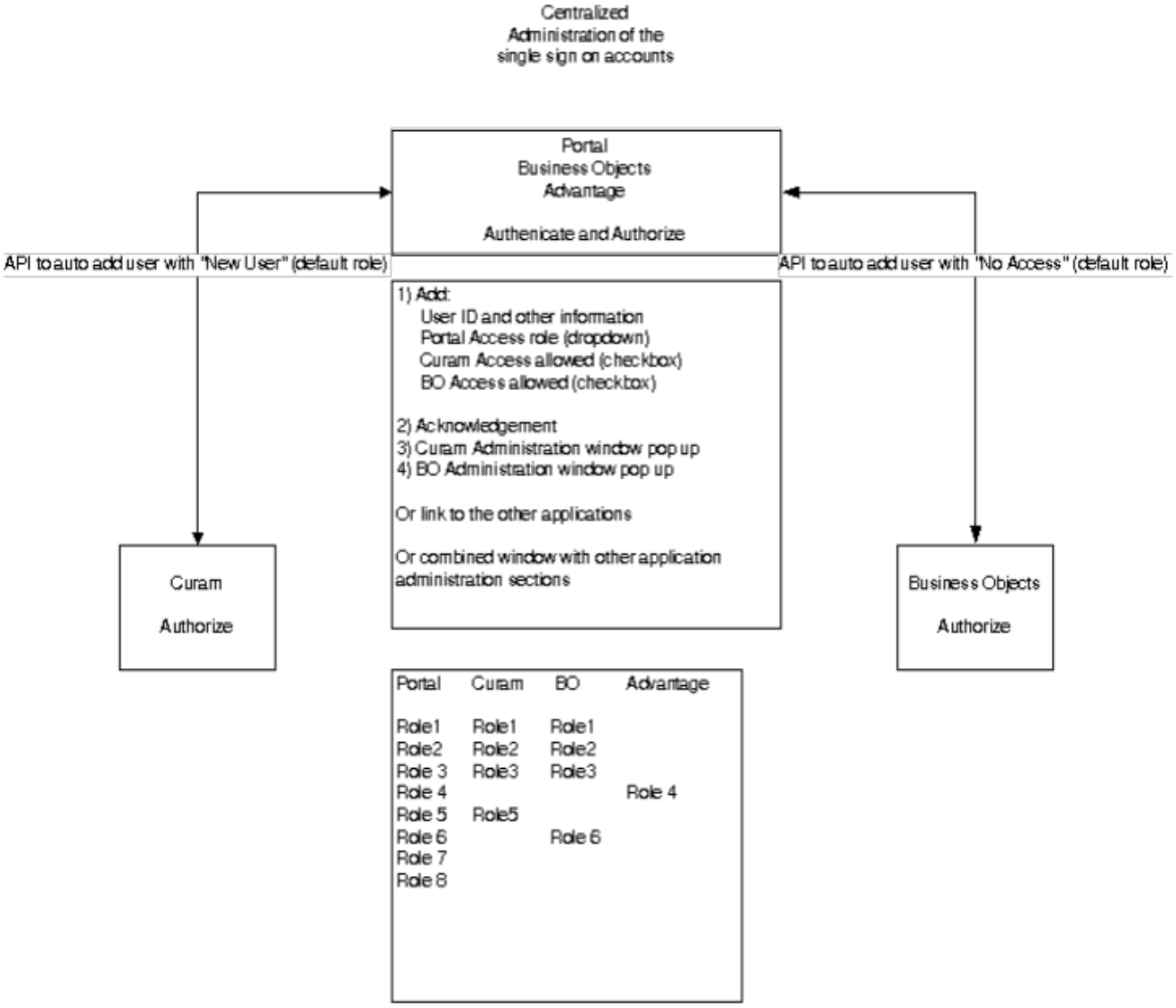


Figure – CMIPS Single Sign-on Diagram

CMIPS uses authentication at the Web Portal for the user and then uses the Web Portal to authenticate into Cúram and BusinessObjects machine to machine.

As described in the above figure, the user logs on to the Web Portal for authentication. The user is authorized to view certain screens and have access to links for Cúram and Business Objects.

As stated in the above figure middle box, when creating a user, the user ID is added to both Cúram and BusinessObjects security with a default role that only allows access to the Home screen of each application. The Web Portal links are displayed based on the role and the user IDs are synchronized with Cúram and Business Objects. Further administration is done within each application by the Security Administrators.

The screens in the Portal such as Security Administration, CMIPS Query and Sampling Tool and Data Retention are controlled by the Portal Security Roles as implemented in the COTS LDAP software and described in sections Web Portal Screen Designs, Navigation Elements and Application Security Roles. Also, additional information can be found in related plans and DSD documentation.

Authorization

CMIPS is using authorization at all three layers of the Web Portal LDAP, Cúram and BusinessObjects so that the specific role a user is assigned authorizes what screens are available and what data is viewable.

Auditing

The portal creates a log entry for each of the following activities:

- Successful login
- Unsuccessful login
- Change in password
- Change in challenge questions and answers
- Failed attempt of using challenge questions
- Successful attempt of using challenge questions
- Change in role
- Change in lockout status
- Change in activation status
- Use of assisted password change

User ID Standards

User ID CMIPS standards:

- Every user name is unique.
- Every user name is traceable to the user.
- User accounts are only disabled and are never deleted in Portal, Case Management, BusinessObjects and CGI Advantage.
- Shall be assigned by a Security Administrator
- Concatenation:
- First name initial
- Last name (seven letters or fewer)
- If required, a three-digit number to make the above combination unique

User Password Standards

CMIPS Password Standards meet minimum requirements per NIST SP 800-43 and OSI-AP-07-03:

- Enforce password history: 10 passwords remembered
- Minimum password length: eight characters
- Passwords must meet the complexity requirements and contain characters from three of the following four categories:
- English upper case characters (A-Z)
- English lower-case characters (a-z)
- Base 10 digits (0-9)
- Non-alphanumeric (such as !,$,#,%)
- Passwords expire every 60 days (Service Accounts [non-human] have 365 days, or if a CMIPS Operations team member leaves CGI before the expiration period or Service Accounts that do not allow expiring password policy will have a non-expiry password)
- Passwords may only be reset once a day excluding the pre-expired initial change
- Pre-expired passwords remain active for 30 days from creation and are randomly generated
- If the account is inactive for 90 days it is deactivated automatically (Service Accounts [non-human] have a 365 day inactive period)
- Account is locked after three failed login attempts
- When any end-user leaves employment with the state or counties, an associated CMIPS Security Officer, per local policy, deactivates that user account

Note: If a team member leaves from the CGI CMIPS Operations staff, all machine passwords are reset as defined in the Operations Manual.

A County Security Officer or his/her designated County Security Administrator is only able to view and manage their respective county accounts. The following exceptions apply:

1. Adding a new user: when conducting a search for verification the account is not already in the CMIPS System as an active or inactive account, the resultant search list is statewide.
2. RE-activating a user: when conducting a search of inactive accounts in the CMIPS System, the resultant search list is countywide.

A special circumstance may exist where one person can perform CMIPS functions for multiple counties. In this case the same person may have multiple user IDs. Each user ID is maintained by the respective county with a unique set of security roles in the Web Portal/LDAP, Cúram (Case Management) and BusinessObjects (reports). This allows each individual county to authorize work functions and processes as per the counties policy and procedures. Each user ID is limited to the restrictions of view ability by county and their security roles. To move between county workspaces, the user would need to log off and log back on. Since the user ID is universal, no connectivity issues exist.

DSD 6/Architecture – System Security/System Security Topic Area/Cúram Security

The following illustrates a high-level flow of CMIPS User authentication and authorization for Case Management within the CMIPS Security Architecture.

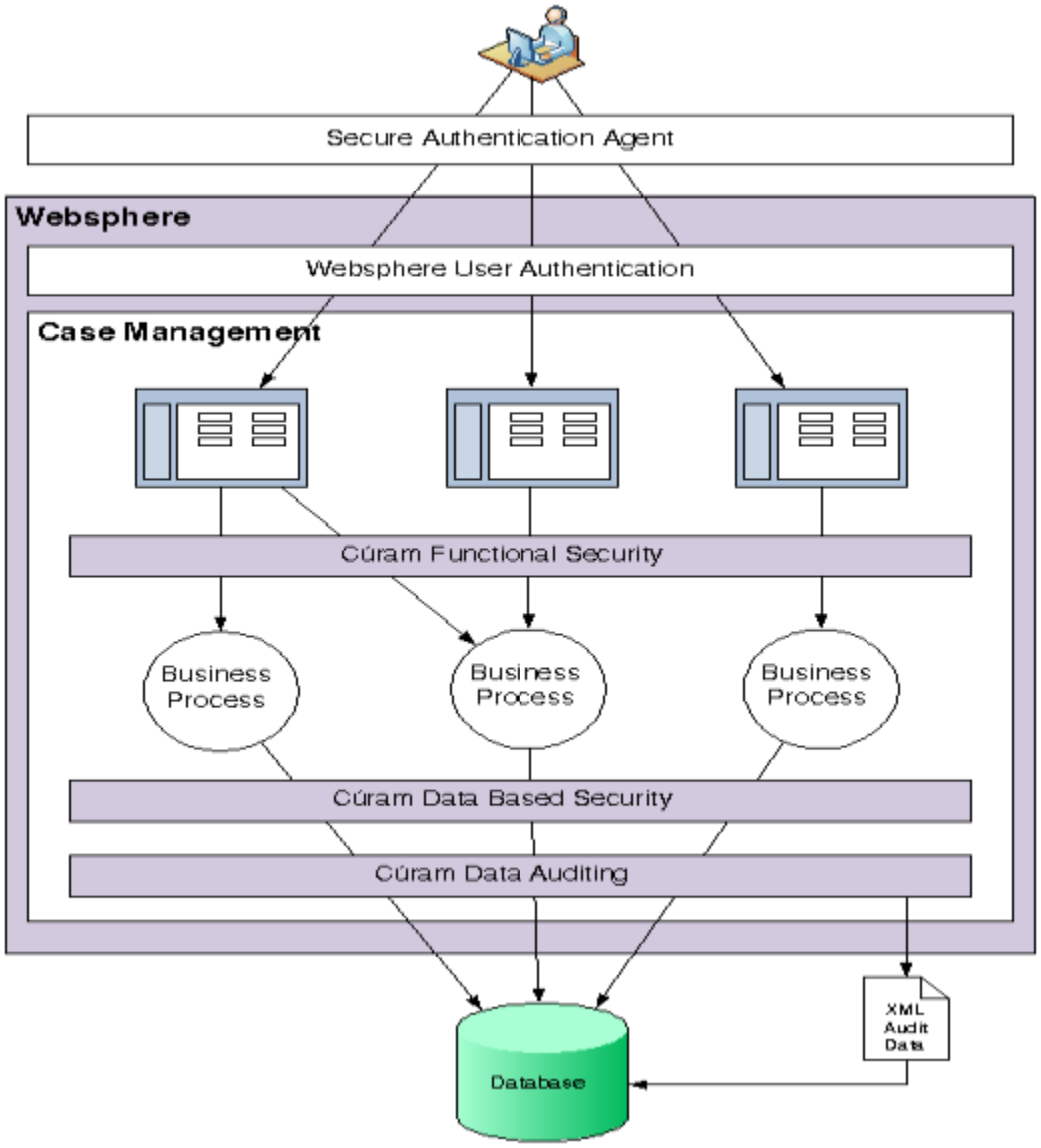


Figure – CMIPS Cúram Security

Cúram facilitates the following security services:

- Authentication
- Authorization
- Role-based security
- Product (program)based security
- Location based security
- Sensitivity-based security
- Field-based security
- Communication/connection security

Authentication (being passed from CMIPS Dynamic Web Portal)

Authentication dictates who can log on to the system through the use of user IDs and passwords. Cúram supports integration with a Lightweight Directory Access Protocol (LDAP) server, whereby the LDAP server can be utilized for password validation, thus facilitating a single point of login across an enterprise network.

Authorization

- Once a user is authenticated via the CMIPS Dynamic Web Portal and machine-to-machine transfer of that authentication to Cúram, it is the responsibility of the Cúram authorization functionality to control access to the various types of securable resources. In Cúram, securable resources include screens, fields, business processes and programs (known as "products" in Cúram). These are controlled through a Security Identifier (SID) that is assigned to each securable feature.
- Each user interface in Cúram is assigned a Function Identifier (FID), which is a specialized form of the SID. The central Cúram UML model controls whether security is enabled for a given user interface and as such the required support code and persistent data is generated automatically. Once security is enabled for a user interface, access is provided to roles rather than individuals. This allows for groupings of individual users according to identified security policy. Using the Cúram Administration Suite, security groups can be created and maintained as changes occur within an organization.
- CMIPS is using Authorization at all three layers of the CMIPS Dynamic Web Portal LDAP, Cúram and BusinessObjects where the specific role assigned authorizes what screens are available and what data is viewable.

Role-Based Security

Cúram utilizes a security hierarchy to define role-based authorization. The root level of the Cúram security hierarchy is the security role assigned to a user. Cúram users are assigned to a security role. This security role determines the functions each user can access, the data they can view and the data they can modify. The role based security is administered in the individual counties based upon the guidelines provided by CDSS and OSI. Cúram meets the HIPAA rule by limiting the access to only those users who are granted the role required to perform their designated duties.

As described above, every business process/function, field, and program available within Cúram is assigned an SID. These SIDs are combined into security groups, which in turn are combined into security roles. A security role within Cúram may have one or more security groups assigned to it. Thus, a logical security role is defined by the combination of security groups, as depicted in the schematic below.

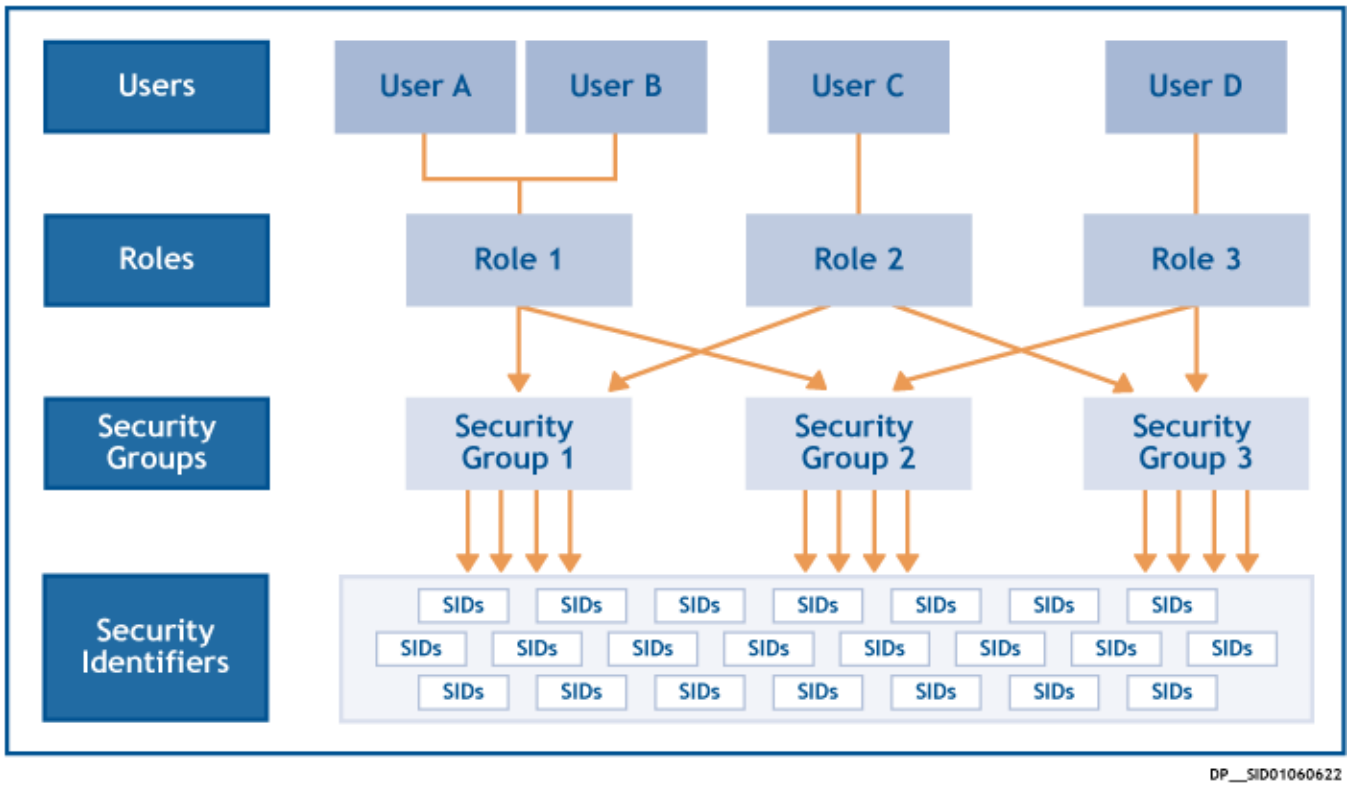


Figure – CMIPSII Cúram Security Hierarchy

High-level view of the Cúram security hierarchy

The Cúram role-based security infrastructure ensures that a suitably secure environment can be deployed to enforce comprehensive authorization and access controls to protect confidential information. In addition to facilitating internal user security controls, Cúram enables selected functions to be made available to clients and other relevant stakeholders. This can be implemented as a secure facility, which requires an external user to be registered on the system and to gain access via a user ID and password. This approach would enable such users to access whatever elements of their own information that an agency chooses to make available, as well as relevant functionality such as inquiry, maintenance of demographic data and other details.

Through its role-based security infrastructure, the comprehensive and customizable Cúram security infrastructure provides the controls necessary to protect client information as required by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

Product-Based Security

As part of the product-based security concept, CMIPS has only installed the Cúram modules (Cúram Enterprise Framework, Cúram Reporting Module, Cúram Administration Suite, Cúram Documentation Suite, Cúram Documentation Toolset and Cúram Financial Module Management) that CMIPS is using. This reduces potential security issues by not having unused products installed. This is similar to removing unused components on a server to reduce security risk, otherwise known as hardening.

Location-Based Security

The locations of a social enterprise organization are the work places of its users. An organization may, for example, define its location types as local offices, district offices or regions. Locations can also be public offices where the public can interact with the organization and there may be multiple locations at the same physical address. Cúram supports location-based security such that user access to case and client information can be limited based on a comparison of the user's location and the location of the case/client information.

Location-based security in Cúram is configured by setting the location data security value on the organization home screen to one of four options: Off, On, Restricted View or Read-Only.

- If Location Data Security is set to "Off" there are no restrictions on users viewing and maintaining case and client information
- If Location Data Security is set to "On" users are only able to view and maintain cases and client information in their own location and sub-locations
- If Location Data Security is set to "Restricted View" users are able to see that a case or client exists in other locations but are not able to view and maintain case or client details outside of their own location
- If Location Data Security is set to "Read-Only" users can view and maintain cases in their own location and sub-locations. Users are able to view client and case information associated with other locations, but are not able to amend or maintain such information. This is the only mode implemented by the CMIPS application.

In addition, location administration can be secured so that only specific users may be assigned the privileges required to update administration details (including security details) for a given location. As for other elements of Cúram security, SIDs is used to determine which users have access to the administrative details for a location.

CMIPS is using location-based security in all three applications, Cúram, BusinessObjects and Web Portal LDAP. Each of the CMIPS user profiles includes the county and/or district office to limit availability of data on screens and reports. Only the specific county user is authorized to take action on their county specific information from a permissible location.

Sensitivity-Based Security

Sensitivity-based security restricts access to what are termed "sensitive" data items. Each data field, work queue and note on the system is designated a sensitivity level.

In order for a worker to have access to the specific data field, work queue, or note, the worker must have an appropriate sensitivity level. This allows the facility to restrict worker's access to sensitive information such as that relating to secure participant types – for example public figures, fellow employees, security forces personnel, and so forth, or to other sensitive participant and case-related data that should be available only to those workers who have an explicit need to access that data.

CMIPS is using the Cúram sensitivity-based security for case notes to further restrict the viewing of associated data within a county and district office.

Field-Based Security

Field-based security governs the user's ability to view information in specific fields. As with FID-based security, the central UML model controls whether security is enabled for a given field. Once security for a field has been enabled and the associated SID added, the new SID may be added to the appropriate user profiles. When field security is in place, only users who have been granted the specified SID may view the field; all other users will see a masked out version of the field.

CMIPS has limited the use of field-based security. In its place, CMIPS has implemented error messages to users trying to access or view unauthorized information or the fields are completely removed from the screen instead of providing grayed out information.

Communication/Connection Security

Encryption of messages/data traffic within CMIPS is facilitated through the Secure Sockets Layer (SSL) protocol, which is configured within the application server product (WebSphere), used in the CMIPS configuration. The level of encryption provided in the CMIPS configuration is determined by a combination of the chosen Web browser and application server products, with 256-bit encryption being used by CMIPS. CMIPS also supports operation over a virtual private network (VPN), if required. Therefore, whether system users are working from a local organization office, or working remotely over VPN, security of data communication is assured.

All CMIPS end-user connections are routed via a DMZ/Web server that reroutes the connection within the DMZ prior to accessing the applications. Full database access is only allowed with machine-to-machine authentication with the application servers and therefore not accessible from any external server to the CMIPS VLAN.

Cúram Auditing

CMIPS Cúram is using comprehensive system auditing and data tracking by maintaining a transparent history of transactions in the Cúram database. This is a feature of Cúram that is implemented against the DB2 tables. The Cúram auditing features provide full before-and-after imaging of records for all inserts, updates and deletes carried out, along with information about both the user and business object (program module or function) that acted on the data. Full details can be restored in the event of hardware or database failure.

The following information is captured by the Cúram auditing service:

- Date and time - the date and time of the transaction
- User ID - the ID of the user who invoked the transaction
- Table name - the name of the database table that was modified
- Program name - the specialized function identifier (FID) of the function that invoked the transaction
- Transaction type - indicates whether the transaction was online, batch or deferred
- Key info - the key that was provided to this operation. Note that this may identify one or many records.
- Details of changed data - these details are logged in an XML format

CMIPS captures and tracks specific audit information for each payment. Detailed information on the destination of payments is provided on the COUNTY PAYMENT VOUCHERS for Recipient and Provider Payments. The source of payments may be tracked in Case Management on the payment transaction history screens (TIMESHEET HISTORY, VIEW PAYMENT CORRECTION AND VIEW SPEC TRANSACTION).

Any further audit information is available within the database. There is no single audit report to track source and destination of the payments in a consolidated view.

Payments to Labor Organizations, Health Benefit Providers, IRS and EDD are maintained within Advantage. Payments to the Labor Organizations and Health Benefit Providers are made via warrants issued by SCO. For Labor Organizations and Health Benefit Providers, the payment information resides in the accounting journal in Advantage Financial. Detail on the Provider deductions that make up those payments resides in Advantage HRM and can be viewed on the LABOR ORG DEDUCTIONS RECONCILIATION report and the BENEFITS DEDUCTIONS RECONCILIATIONS report. Payments to the IRS and EDD are made via funds transfer. Payment information resides in the accounting journal in Advantage Financial on a JVA (Journal Voucher Advanced) document. Detail for these payments can be viewed on the QUARTERLY FEDERAL TAX DISBURSEMENT SUMMARY REPORT and the QUARTERLY STATE TAX DISBURSEMENT SUMMARY REPORT. These reports are used to create the Federal Tax Memo and the State Tax Memo which CDSS Accounting uses to initiate the funds transfer.

Audit data is processed and sent to the Report Database to support investigations or problem analysis. In addition, where a certain audit event occurs, workflow events are raised to perform certain actions, such as to generate an alert to a designated user for appropriate action to be taken. Some alerts are programmed into CMIPS via the Case Management DSD (Detail System Design) and may be updated as lessons learned determine additional audit events. The root cause analysis, which includes lessons learned, is defined in the Customer Service Plan.

Defining CMIPS Cúram Application Security

The CMIPS project defined the security structure via the requirements and functionality list identified for the implementation in conjunction with the Case Management DSD.

- Identify Security Roles
- Every authorized Cúram user is assigned a security role; therefore, it is possible to authorize every user against any secured element of an application
- These security roles are at the top level of the security identifier hierarchy
- Security roles are mapped to individual screens
- Security roles were also compared to other security functionality such as Location, Position, Queues, and Workflow
- Identify Security Groups
- The security group level involves the grouping together of related SIDs, which includes business functions and screens.

DSD 6/Architecture – System Security/System Security Topic Area/BusinessObjects Security

BusinessObjects security operates in a similar fashion to Cúram Security. The initial setup of a user role is accomplished via an API from the Web Portal to BusinessObjects with a default role. The CMIPS Security Office or Administrator then logs onto Business Objects, assigns an appropriate security profile, and validates/updates security profile information. The data visible to the end-user while running reports is determined by a combination of a security role, the reports the user has access to, and other profile data, such as county, for the data in those reports.

For more detail on the security roles for BusinessObjects, refer to Security Roles section, and associated Case Management, Payroll, or Funds Management DSD sections. A summary of all reports is located in the Reporting Database DSD for a cross reference as to which DSD document to reference.

Basic design philosophy on security roles for BusinessObjects reports listed in the System Security Plan (CMIPShare > Document Center > Deliverables > 6.7-01 System Security Plan) are:

- If a user can see the data in Case Management then the user should have access to the associated reports
- If a user can see the data in Payroll and Funds Management then the user should have access to the associated reports
- If a user needs access to the information to perform analysis or program management, then the user should have access to the associated reports
- If a user is responsible for maintaining the data security (e.g. the user is a Security Officer) then the user should have access to the associated reports

BusinessObjects Folder and Report Security

BusinessObjects security operates in a similar fashion to Cúram Security. The initial setup of a user role is accomplished via an API from the CMIPS Dynamic Web Portal to BusinessObjects with a default role. The CMIPS Security Office or Administrator then logs onto Business Objects, assigns an appropriate security profile, and validates/updates security profile information. The data visible to the end-user while running reports is determined by a combination of a security role, the reports the user has access to, and other profile data, such as county, for the data in those reports.

For more detail on the security roles for BusinessObjects, refer to Security Roles section, and associated Case Management, Payroll, or Funds Management DSD.

Basic design philosophy on security roles for BusinessObjects reports listed in the System Security Plan (CMIPShare > Document Center > Deliverables > 6.7-01 System Security Plan) are:

- If a user can see the data in Case Management then the user should have access to the associated reports
- If a user can see the data in Payroll and Funds Management then the user should have access to the associated reports
- If a user needs access to the information to perform analysis or program management, then the user should have access to the associated reports

If a user is responsible for maintaining the data security (e.g. the user is a Security Officer) then the user should have access to the associated reports

Folder	Groups Assigned to Folder	Access Level
Case Maintenance		
	CMIPSII_Core	View On Demand
	CMIPSII_InternalHP	View On Demand
	CMIPSII_StateOnly	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Data Download		
	CMIPSII_County_Admin	View On Demand
	CMIPSII_InternalHP	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Data Retention		
	CMIPSII_County_Admin	View On Demand
	CMIPSII_InternalHP	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS

Health Benefit Managers		
	CMIPSII_HealthBenefitMgrs	View On Demand
	CMIPSII_InternalHP	View On Demand
	CMIPSII_StateOnly	View On Demand
	Administrators– This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Homemaker Reports		
	CMIPSII_Core	View On Demand
	CMIPSII_InternalHP	View On Demand
	CMIPSII_StateOnly	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Labor Organizations		
	CMIPSII_LaborOrganizations	View On Demand
	CMIPSII_StateOnly	View On Demand
	CMIPSII_InternalHP	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Ops_HelpDesk		
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	HelpDesk	View On Demand
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Payroll		
	CMIPSII_Core	View On Demand
	CMIPSII_InternalHP	View On Demand
	CMIPSII_StateOnly	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Provider Management		
	CMIPSII_Core	View On Demand
	CMIPSII_InternalHP	View On Demand
	CMIPSII_StateOnly	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
QA/Fraud		
	CMIPSII_Core	View On Demand
	CMIPSII_InternalHP	View On Demand
	CMIPSII_StateOnly	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Shared Reports Folder		

	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
State Only		
	CMIPSII_InternalHP	View On Demand
	CMIPSII_StateOnly	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
System Performance		
	CMIPSII_County_Admin	View On Demand
	CMIPSII_InternalHP	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
System Security		
	CMIPSII_County_Admin	View On Demand
	CMIPSII_InternalHP	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Temporary Storage		
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
Time and Attendance		
	CMIPSII_Core	View On Demand
	CMIPSII_InternalHP	View On Demand
	CMIPSII_StateOnly	View On Demand
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
User Folders		
	Administrators – This is not a standard group that can be selected, but a logical group for descriptive purposes	Full Control
	Everyone – This is not a standard group that can be selected, but a logical group for descriptive purposes	NO ACCESS
WPCS		
	CMIPSII_WPCS	View On Demand
	CMIPSII_InternalHP	View On Demand
	CMIPSII_StateOnly	View On Demand
	Administrators	Full Control
	Everyone	NO ACCESS

BusinessObjects Universe and Universe Connection Security

The universes and universe connections that are defined in the BusinessObjects environment require the "View On Demand" security level in order to successfully execute reports in an on-demand fashion. Therefore, the "Everyone" group has been defined with the "View On Demand" to simplify the security model.

BusinessObjects Filter-Based Report Data

The security for reports and folders defined in the "BusinessObjects Folder and Report Security" section, allows users access to view and run reports. However, this alone does not limit the scope of the data available to the user. More security is added by using a filter that is defined within the reports. During creation of the user in the CMIPS Web Portal, additional information must be supplied to properly create a user. This detail includes, but is not limited to, data such as the user's county affiliation and the "data view ability" which can be one of three levels: State level, County level or Worker level. When a report is run on-demand or as scheduled, the report logic compares the user's county as well as the "data view ability" to determine the data that is returned to the user. This ensures that users have access only to the data that they are authorized to view.

BusinessObjects Account Management

Once a user is defined for authorized access to reports in the CMIPS Web Portal application, the user account becomes available to be assigned to security groups listed below in the BusinessObjects infrastructure.

- CMIPSII_Admin
- CMIPSII_Core
- CMIPSII_InternalHP
- CMIPSII_HealthBenefitMgrs
- CMIPSII_LaborOrganizations
- CMIPSII_StateOnly
- CMIPSII_WPCS

Delegation of adding or removing users from the above groups is assigned to users that are defined in the CMIPS Help Desk security group. Users associated with the CMIPS Help Desk group cannot add or remove themselves or other users into this security group. Any changes to this group membership require a user defined in the BusinessObjects Administrators group.

DSD 6/Architecture – System Security/System Security Topic Area/Advantage Security

CGI staff creates Advantage user IDs and assigns the appropriate role when a request, received by the CMIPS Help Desk, is forwarded to CGI. This process is defined in the Help Desk manual section named "Advantage User."

DSD 6/Architecture – System Security/System Security Topic Area/Other LDAP Security Programs

CMIPS Dynamic Web Portal LDAP security is also integrated with CGI Advantage, ServiceNow, Web Sphere middleware, DB2, Business Process Server and other associated programs like AutoSys, LIMS, and Universal Addressing Module Software-as-a-Service, etc. The programs all use LDAP for authentication but each has a unique branch for authorization in an integrated LDAP tree structure. The roles used by the CMIPS Dynamic Web Portal also control the security authorizations of the other applications primarily around system administration and program management. Refer to CMIPS Dynamic Web Portal Security Roles outlined in the Application Security Roles section. More specific detail is included in the associated Customer Service Plan and the Operations Manual.

DSD 6/Architecture – System Security/Business Processes

CMIPS screen security is controlled based upon predefined security roles. Each CMIPS screen is associated with one or more security roles. These security roles are defined to control access to specific screens as well as the level of access (read or update) within a specific screen.

DSD 6/Architecture – System Security/Business Processes /Business Process Functions

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/Log On for Every User

CI	Document Name
CI-67083 - DSD SF Log On for Every User IMPLEMENTED	DSD_SF_Log_On_for_Every_User.doc

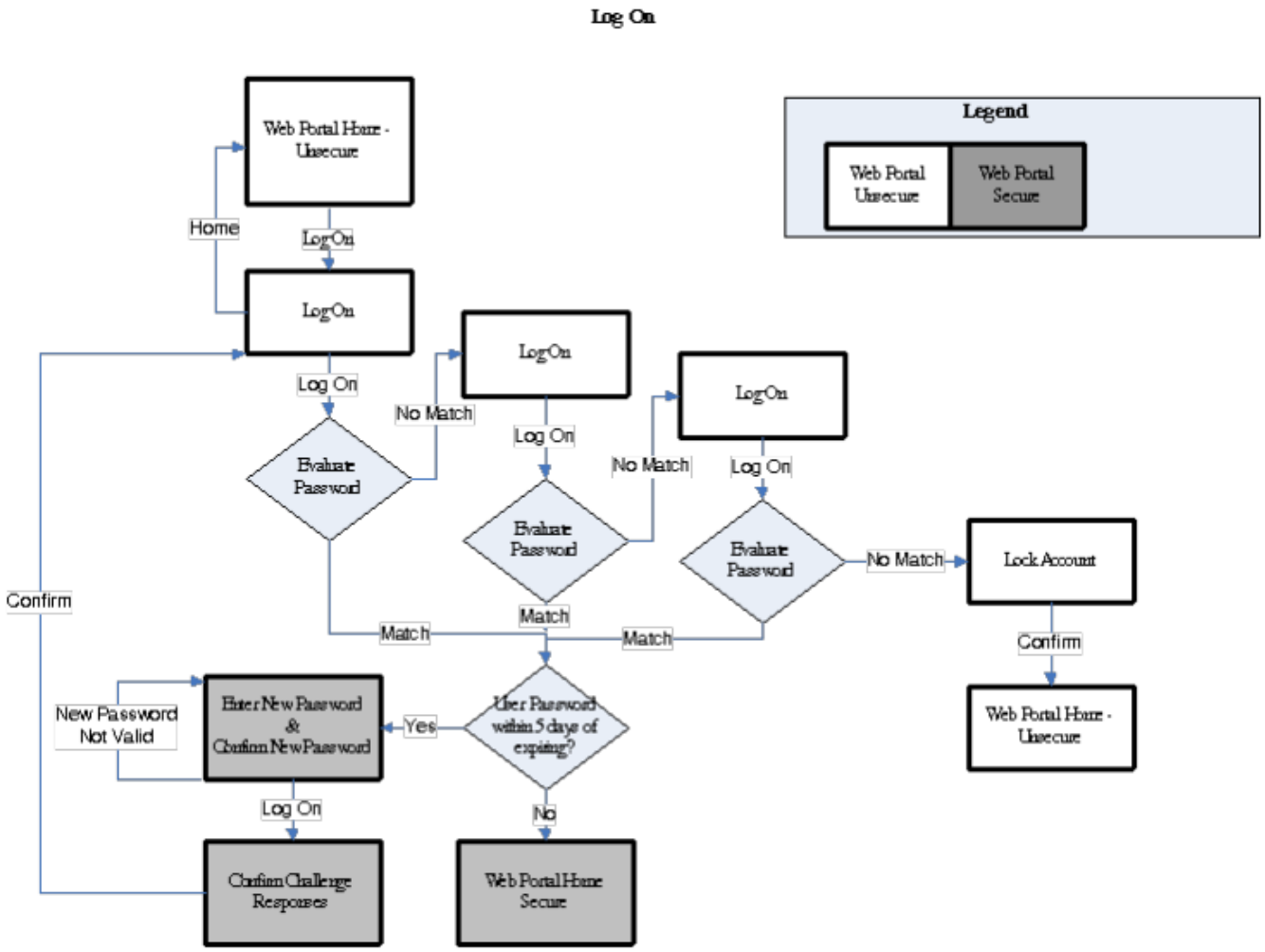


Figure – Log On Business Process Flow

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/Reset Password from Unsecured side of Web Portal (via Challenge)

CI	Document Name
CI-67078 - DSD SF Reset Password from Unsecured side of Web Portal (via challenge) IMPLEMENTED	DSD_SF_Reset_Password_from_Unsecured_side_of_Web_Portal_(via_challenge).doc

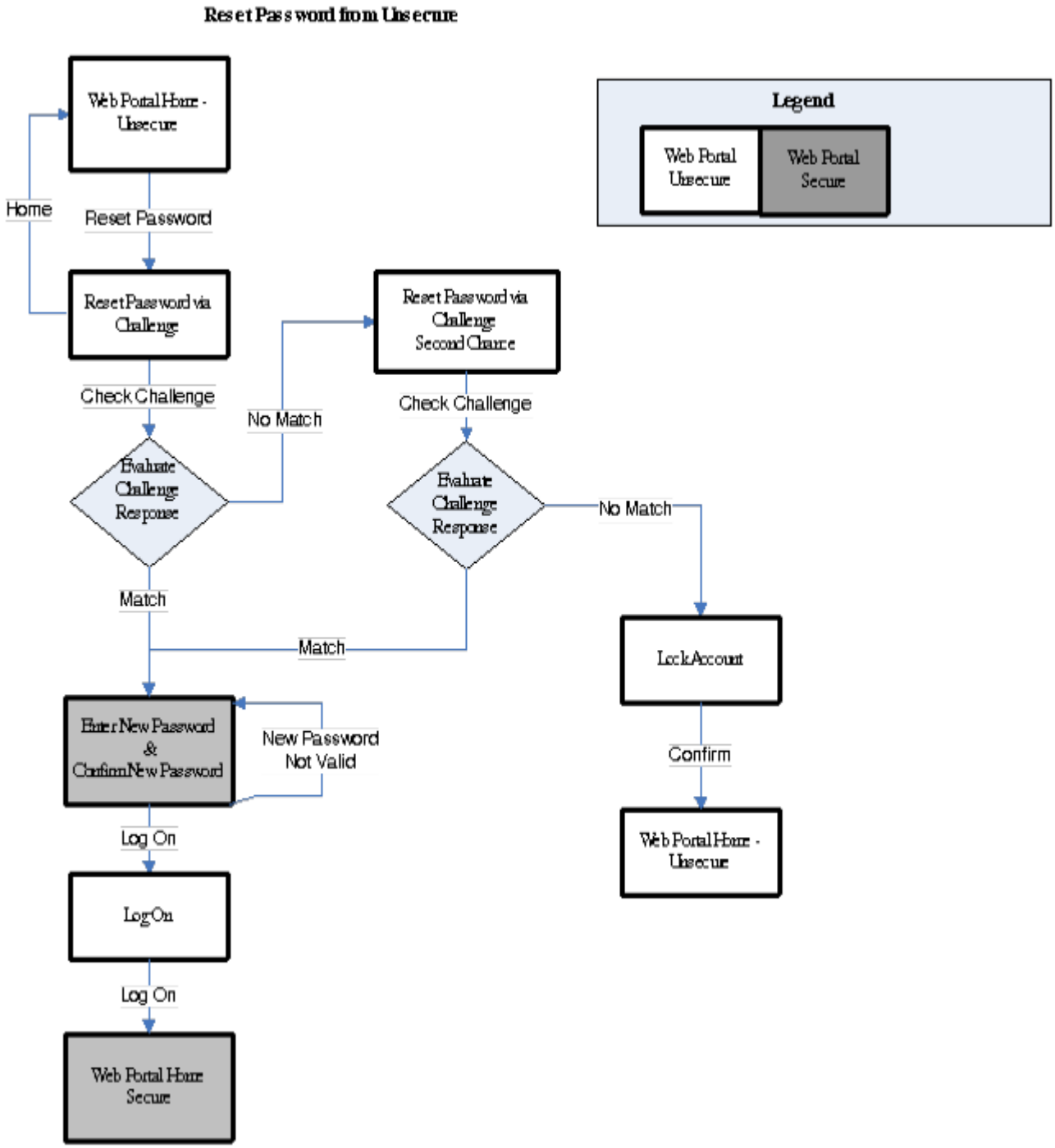


Figure – Reset Password Flow

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/Reset Password After Successful Log On

CI	Document Name
CI-67087 - DSD SF Reset Password after successful Log On IMPLEMENTED	DSD_SF_Reset_Password_after_successful_Log_On.doc

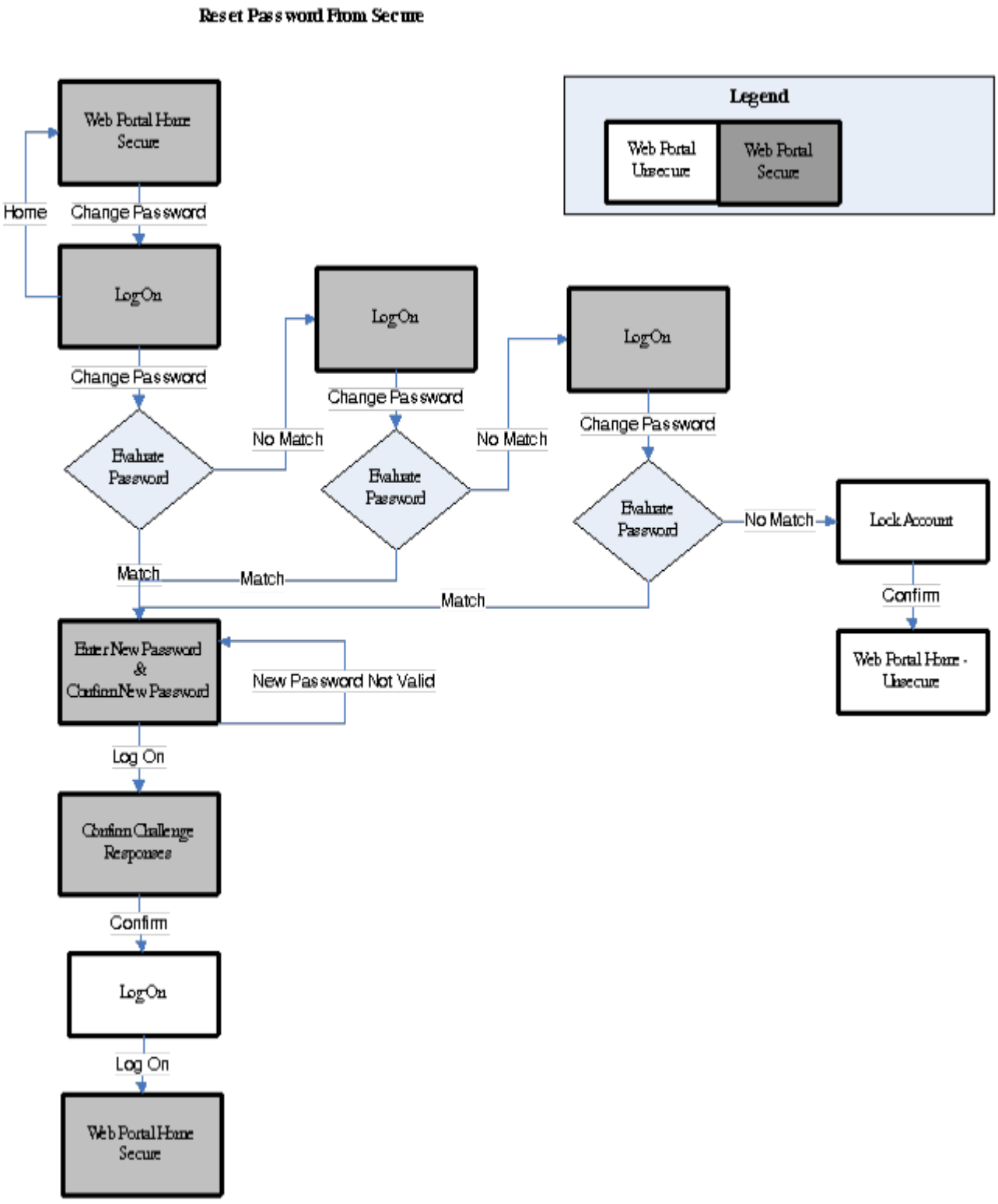


Figure – Reset Password After Log On

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/Maintain Account Information

CI	Document Name
CI-67081 - DSD SF Maintain Account Information by User IMPLEMENTED	DSD_SF_Maintain_Account_Information_by_User.doc

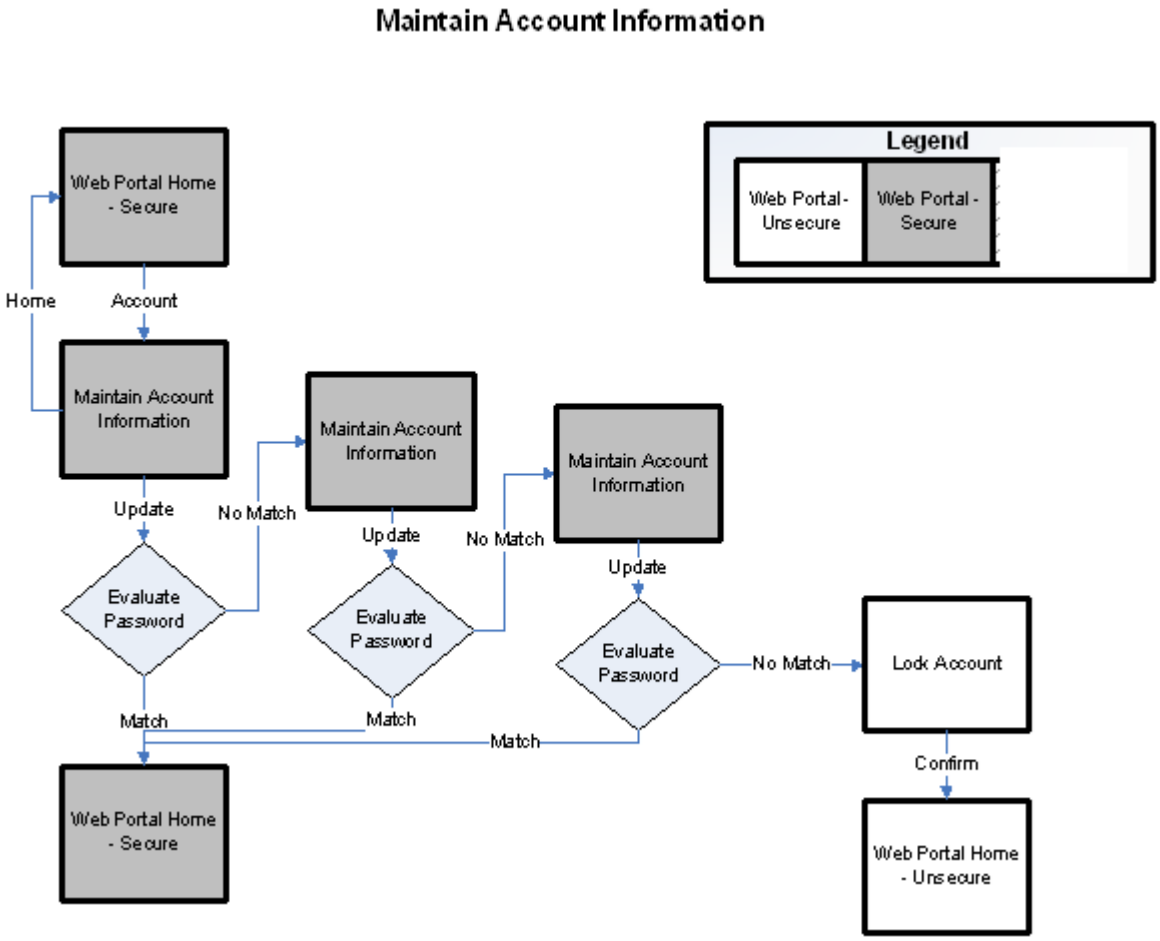
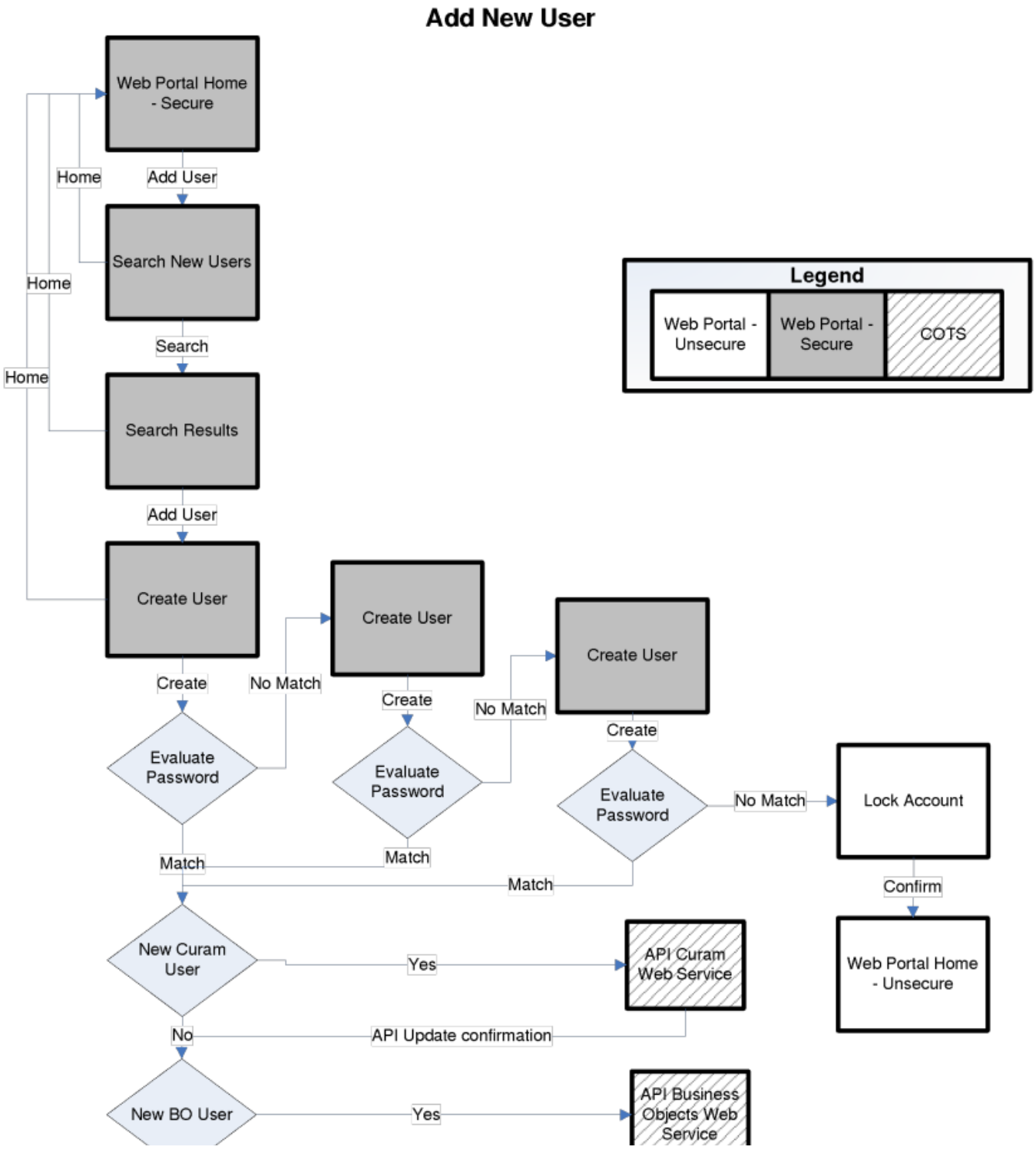


Figure – Maintain Account Information by User

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/Add New User by Security Officer

CI	Document Name
CI-67085 - DSD SF Add new user by Security Officer IMPLEMENTED	DSD_SF_Add_new_user_by_Security_Officer.doc



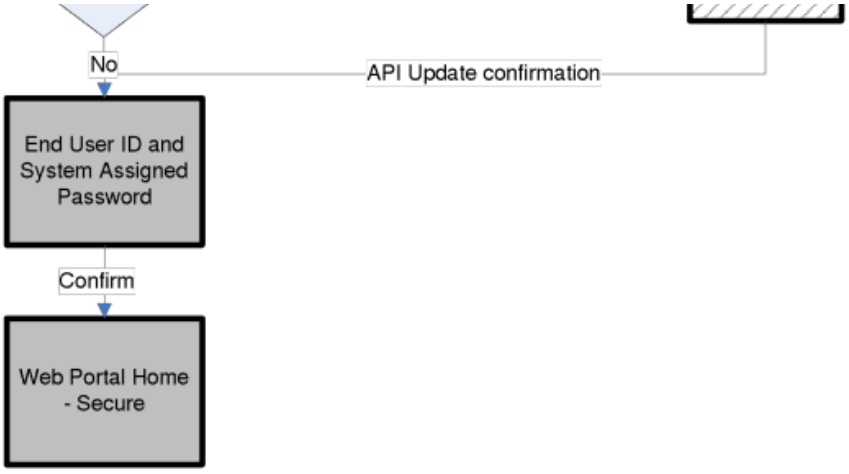


Figure – Add New User

Note: Search is statewide based on search criteria.

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/Update Portal Profile by Security Administrator

CI	Document Name
CI-67080 - DSD SF Update Portal Profile by Security Administrator IMPLEMENTED	DSD_SF_Update_Portal_Profile_by_Security_Administrator.doc

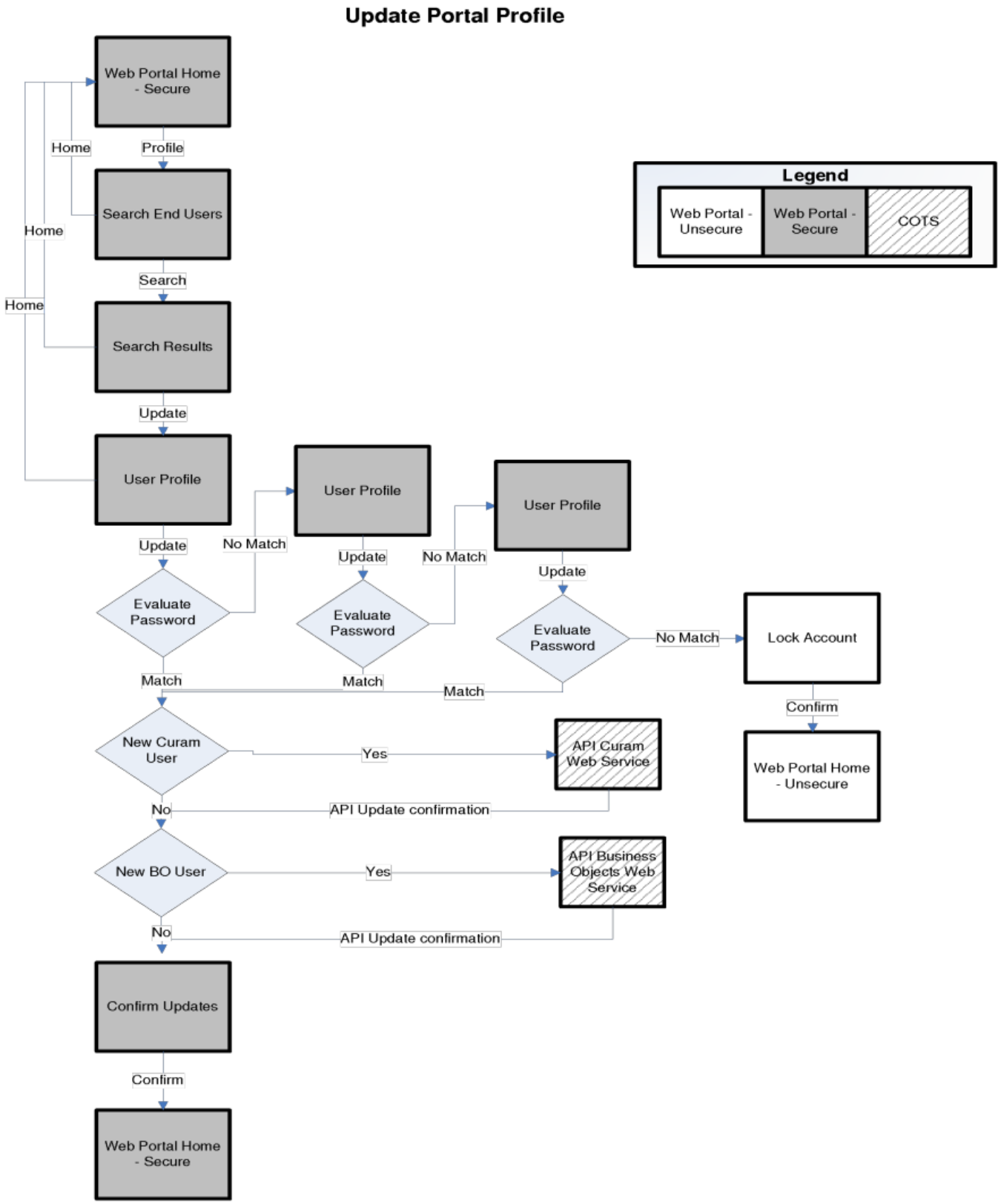


Figure – Update Portal Profile

Note: Search is limited to county user accounts of the respective county of the County Security Officer or County Security Administrator.

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/First Time Log On by a User

CI	Document Name
CI-67082 - DSD SF First Time Log On by a user IMPLEMENTED	DSD_SF_First_Time_Log_On_by_a_user.doc

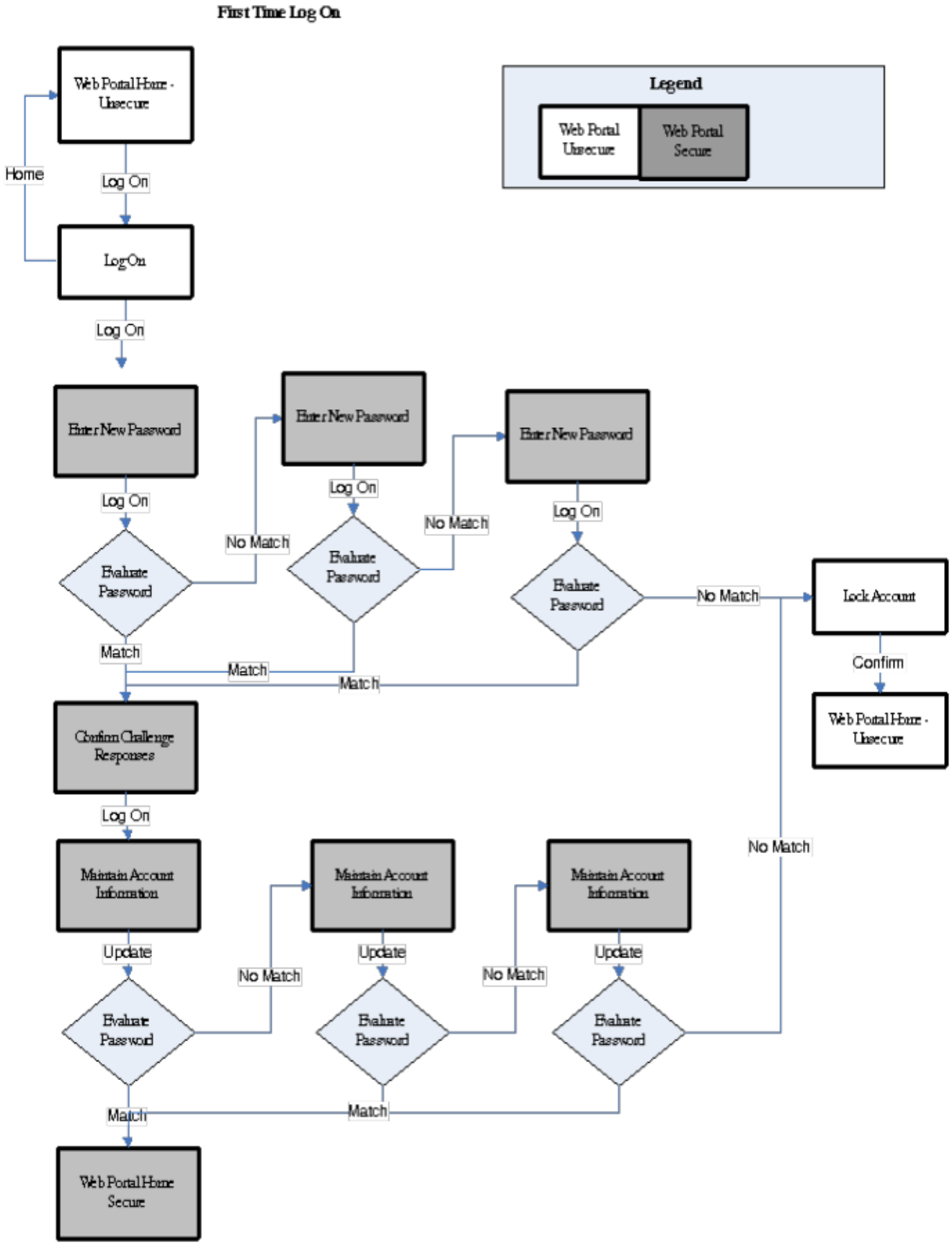


Figure – First Time Log On

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/Reset Password with Assistance from Security Administrator or Help Desk

CI	Document Name
CI-67079 - DSD SF Reset Password with assistance from Security Administrator or Help Desk IMPLEMENTED	DSD_SF_Reset_Password_with_assistance_from_Security_Administrator_or_Help_Desk.doc

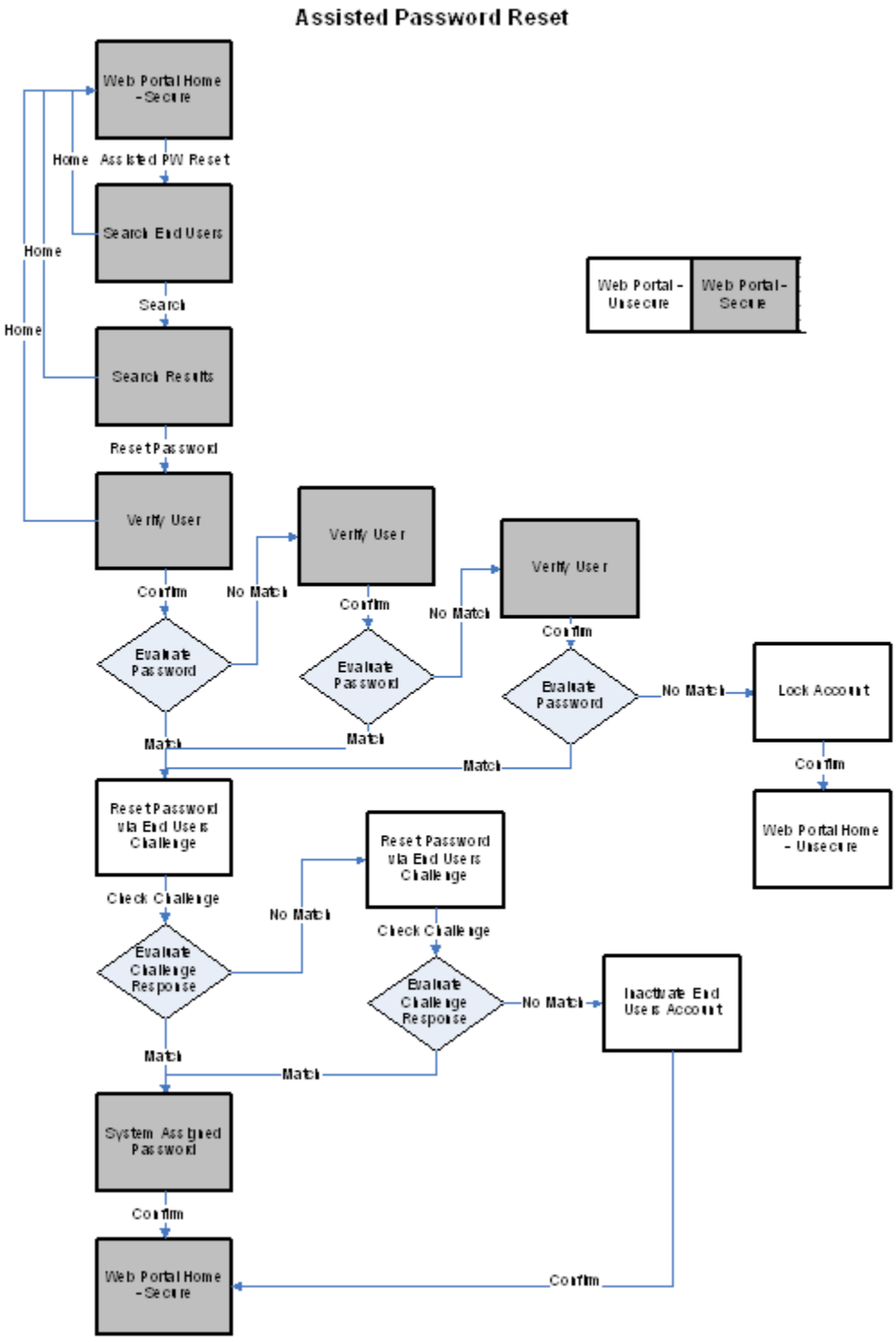


Figure – Reset Password with Assistance

Note: Search is limited to county user accounts of the respective county of the County Security Officer or County Security Administrator.

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/Deactivate a User Account

CI	Document Name
CI-67086 - DSD SF Deactivate a User Account IMPLEMENTED	DSD_SF_Deactivate_a_User_Account.doc

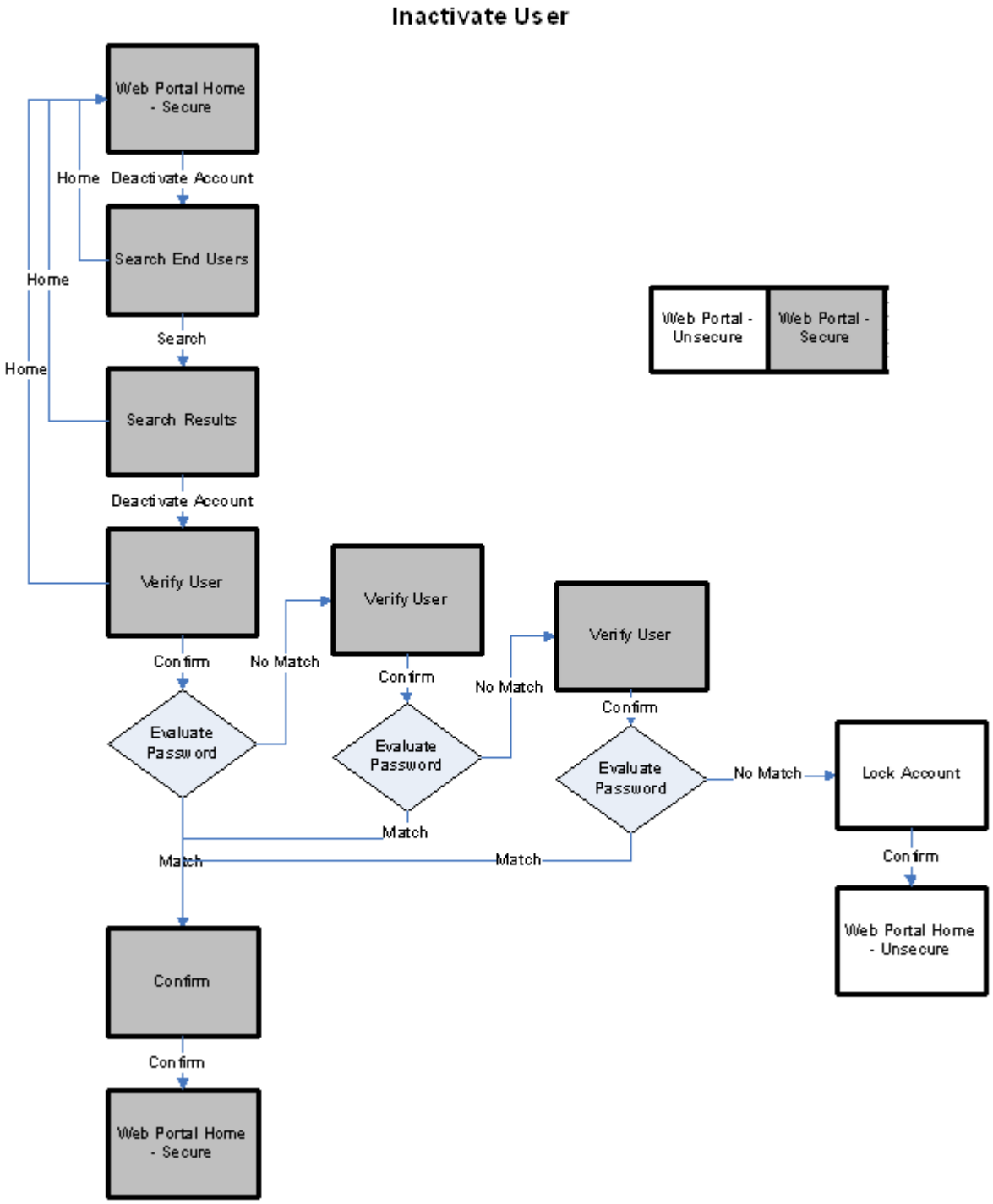


Figure – Deactivate a User Account

Note: Search is limited to county user accounts within the respective county of the County Security Officer or County Security Administrator.

DSD 6/Architecture – System Security/Business Processes /Business Process Functions/Activate a User Account

CI	Document Name
CI-67084 - DSD SF Activate a User Account IMPLEMENTED	DSD_SF_Activate_a_User_Account.doc

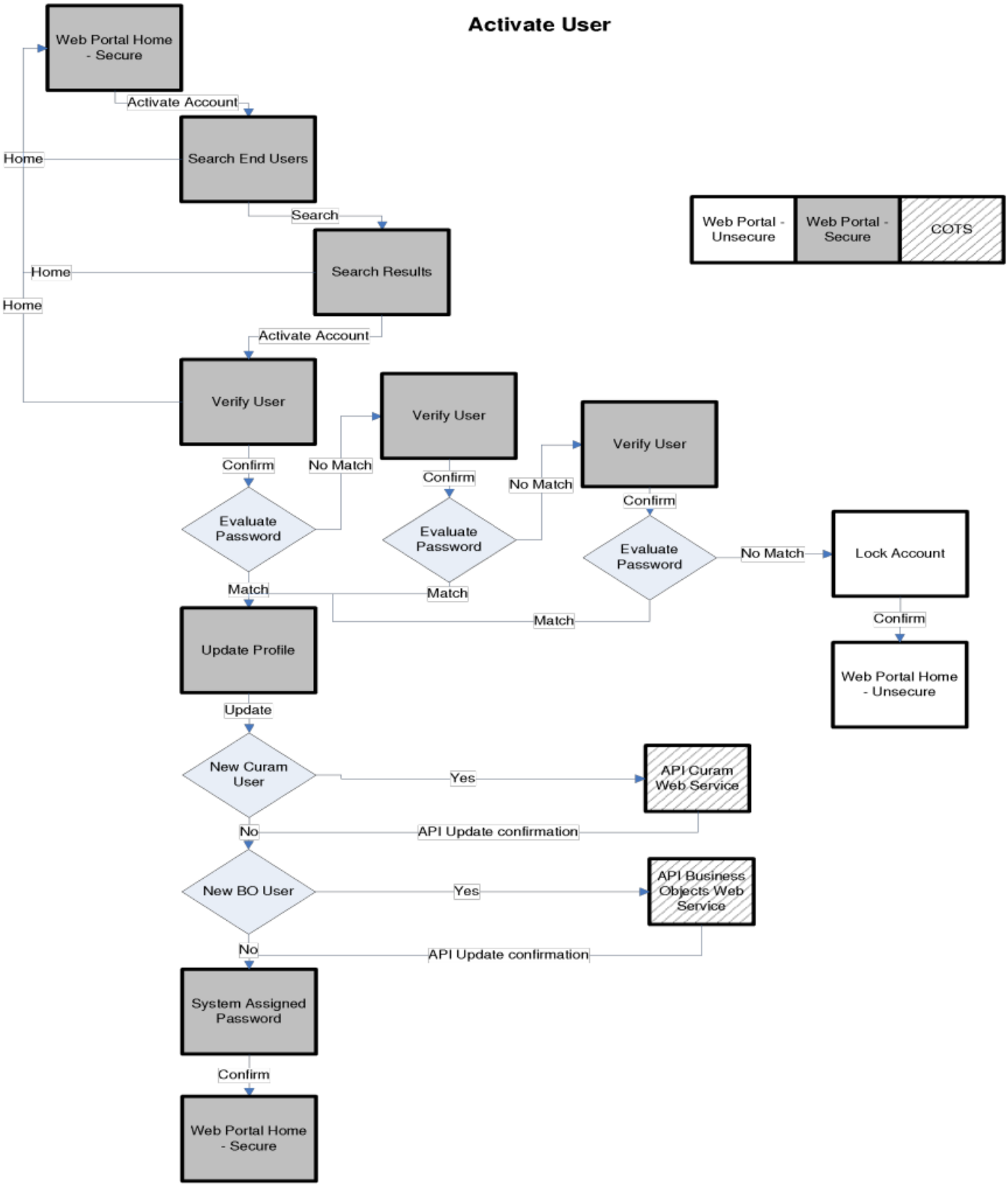


Figure – Activate a User Account

Note: Search is limited to user accounts within the respective county of the County Security Officer or County Security Administrator.

DSD 6/Architecture – System Security/Business Processes /Screen Designs

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Cúram Screens Related to Security Structure

Cúram security screens can be found in the Program Management and Fraud DSD Section.

DSD 6/Architecture – System Security/Business Processes /Screen Designs/BusinessObjects Screens

DSD 6/Architecture – System Security/Business Processes /Screen Designs/BusinessObjects Screens/Log into CMC using Administrator ID and Password

CI	Document Name
CI-116572 - DSD SC CMC Administration IMPLEMENTED	DSD_SC_CMC_Administration.doc

Figure – CMC Administration

Hyperlinks/Functions

The following hyperlink functionality is associated with the CMC Administration screen:

Hyperlink	Function
Log On	Authenticate user

Data Elements

The following data elements are specific to the CMC Administration screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
System	Default configuration information for CMC	URL and Port Path	Yes	No	Yes
User Name	CMIPS User ID	Text	Yes	No	Yes
Password	User-entered password	String	Yes	No	Yes
Authentication Type	Type of authentication	Text	Yes	Yes	No

DSD 6/Architecture – System Security/Business Processes /Screen Designs/BusinessObjects Screens/Folders

CI	Document Name
CI-116582 - DSD SC Folders IMPLEMENTED	DSD_SC_Folders.doc

Selected Folder shows all of the reports and its subfolders (if any)

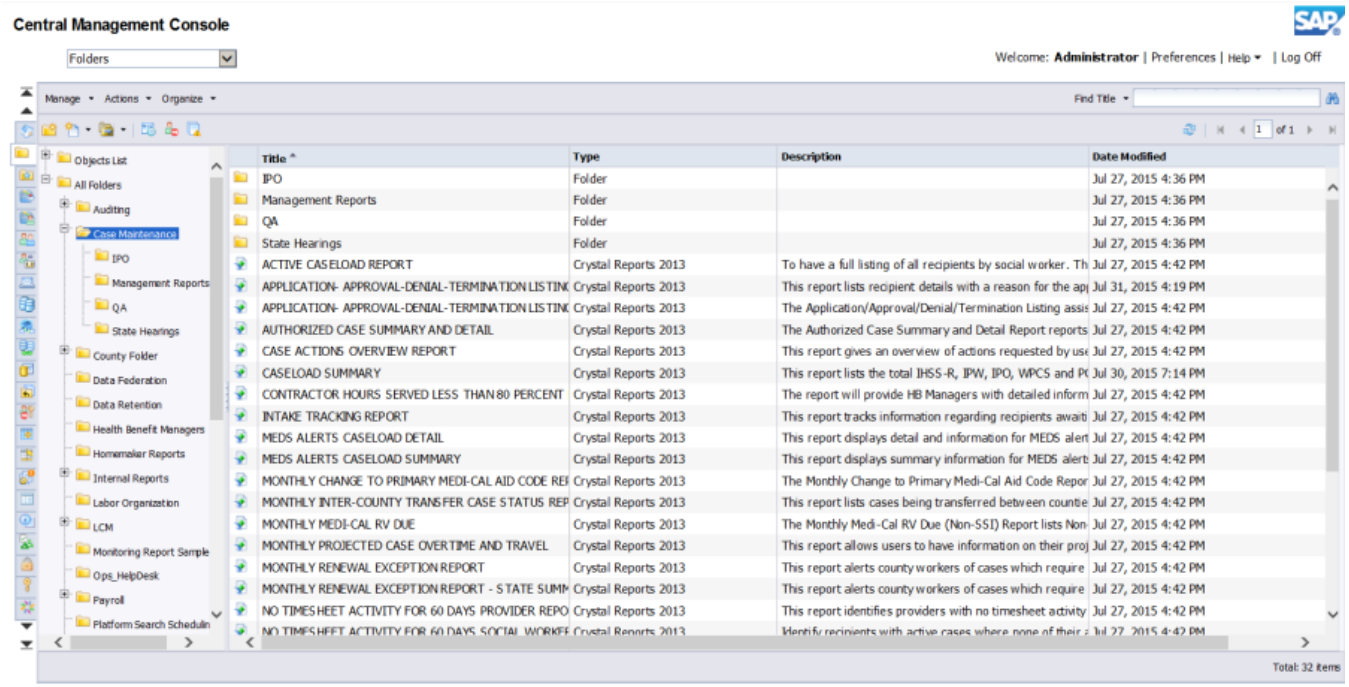


Figure – Folders

Hyperlinks/Functions

The following hyperlink functionality is associated with the Folders Screen:

Hyperlink	Function
<Report Name>	This link allows users to view report details

Data Elements

None

DSD 6/Architecture – System Security/Business Processes /Screen Designs/BusinessObjects Screens/User Security

CI	Document Name
CI-116589 - DSD SC User Security IMPLEMENTED	DSD_SC_User_Security.doc

The User Security allows the Administrator to set folder level permissions.

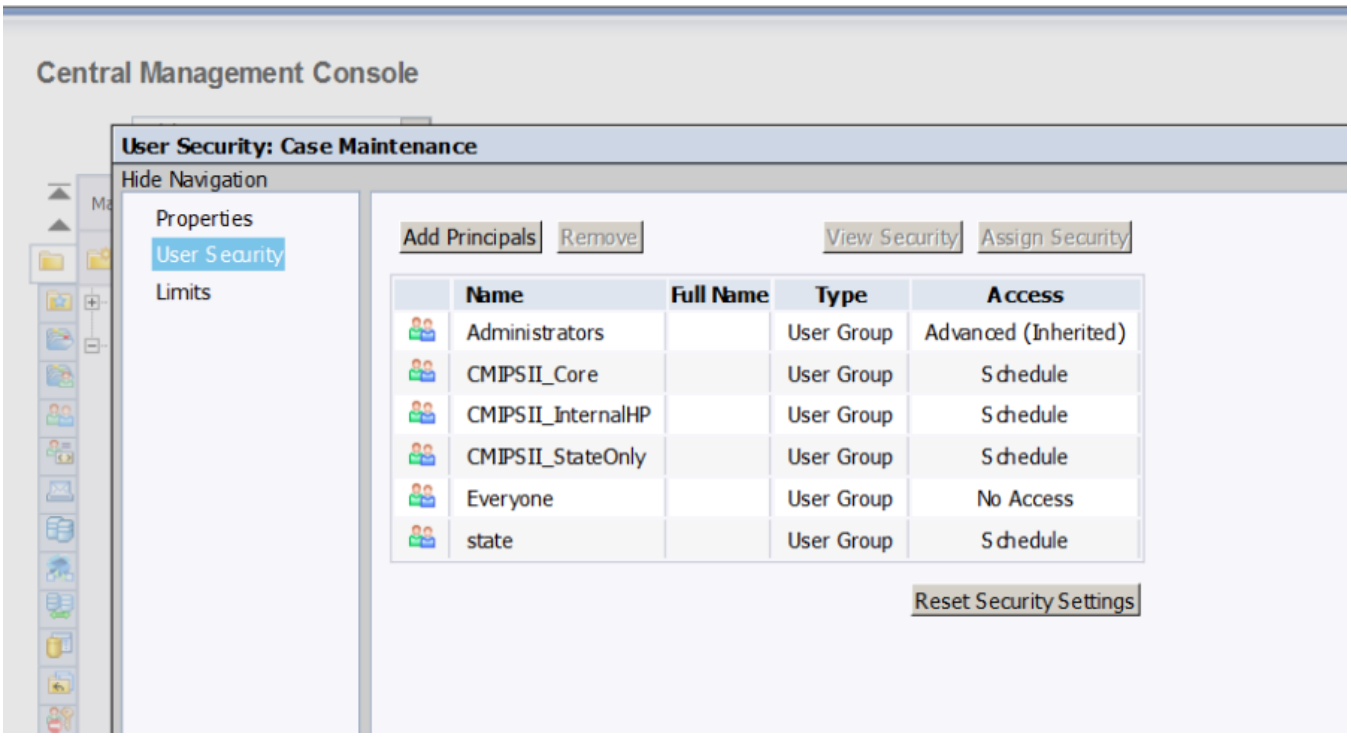


Figure – User Security

In this screen example, Report View and Refresh was added. An administrator can update the Access Level rights as documented above.

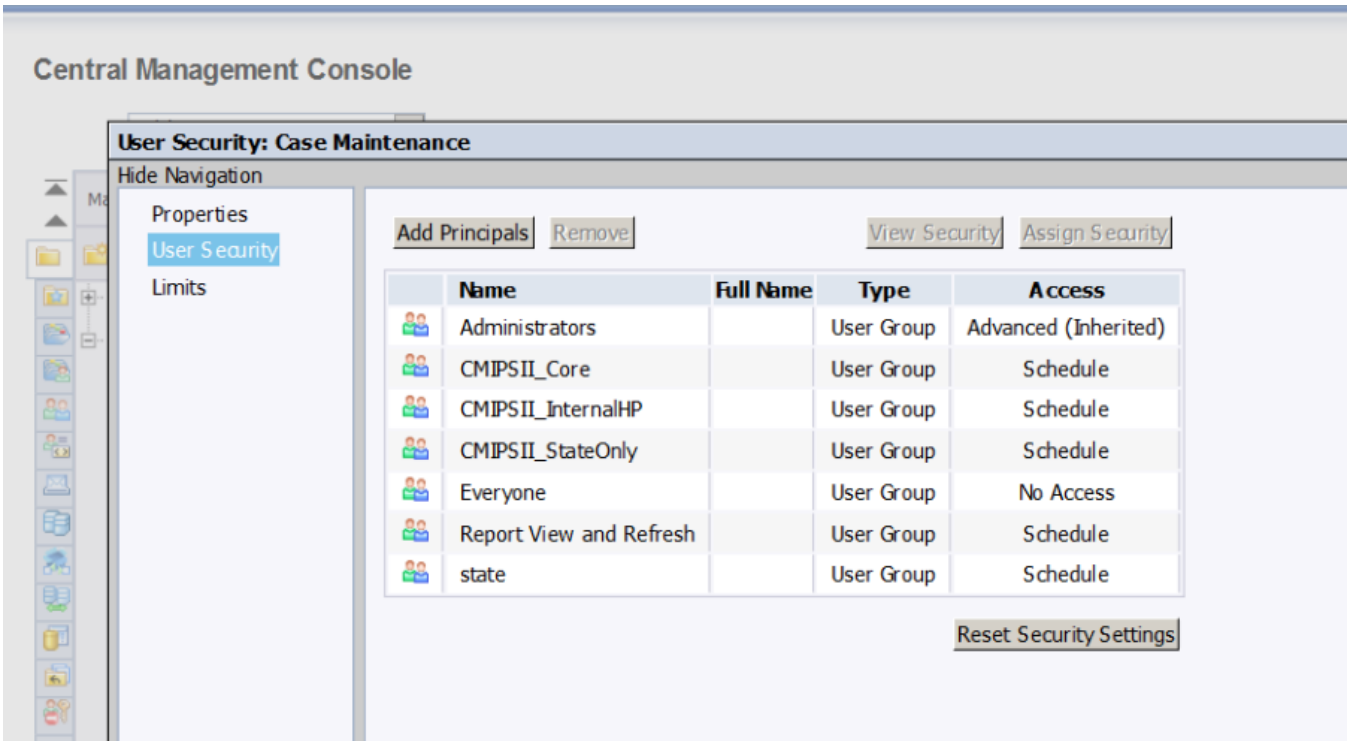


Figure – User Security – Update Example

DSD 6/Architecture – System Security/Business Processes /Screen Designs/BusinessObjects Screens/Assign Security – Access Levels

CI	Document Name
CI-116588 - DSD SC Assign Security Access Levels IMPLEMENTED	DSD_SC_Assign_Security_Access_Levels.doc

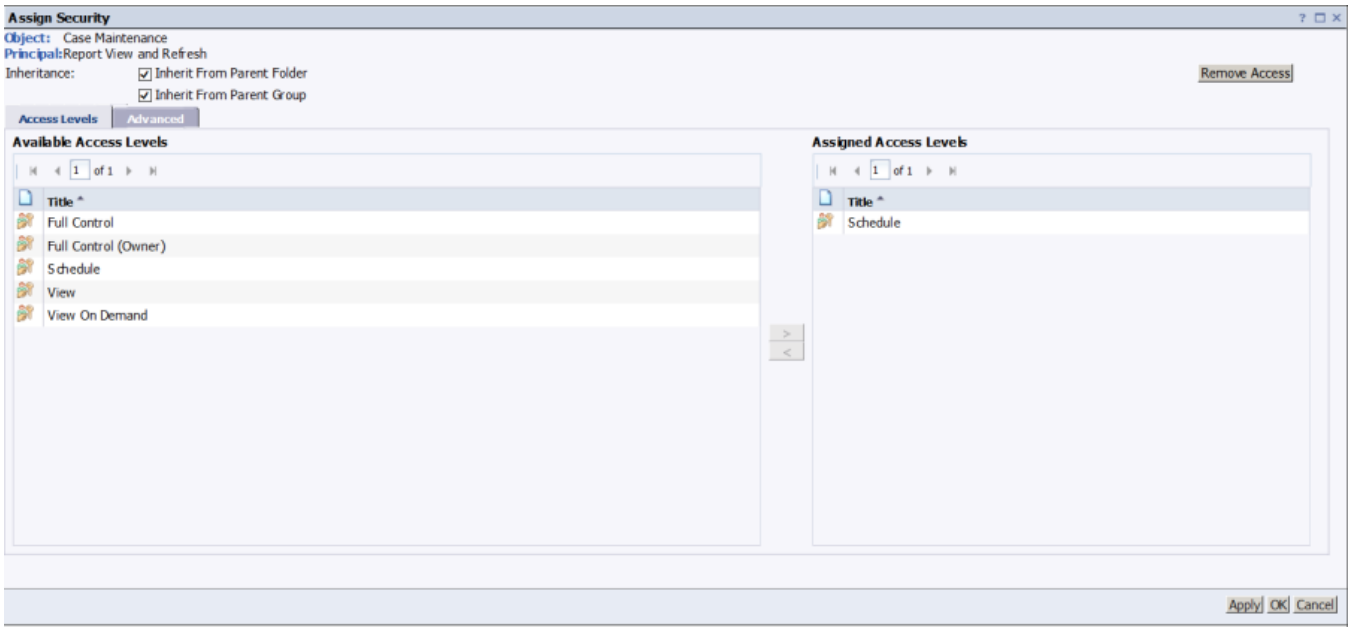


Figure – Assign Security – Access Levels

Hyperlinks/Functions

The following hyperlink functionality is associated with the User Security screen:

Hyperlink	Function
Add Principals	Allows the addition of groups and users
Remove	Removes the access to the selected folder for the selected group
View Security	Allows to view the security to the selected folder for the selected group
Assign Security	Allows to assign the Access Levels
Reset Security Settings	Reset to previously saved values

The following hyperlink functionality is associated with the Access Levels screen:

Hyperlink	Function
Apply	Saves and applies but stays on same screen.
Ok	Saves and applies changes and returns to previous screen.
Cancel	Returns to previous page.

Data Elements

None

DSD 6/Architecture – System Security/Business Processes /Screen Designs/BusinessObjects Screens/Advanced Rights

CI	Document Name
CI-116567 - DSD SC Assign Security Advanced IMPLEMENTED	DSD_SC_Assign_Security_Advanced.doc

From the User Security, select the group, click on the "Assign Security", click on "Advanced" tab and then click on "Add/Remove Rights". A wide variety of rights can be explicitly granted or denied. Most of these rights should be explicitly denied to prevent general users from modifying the reports.

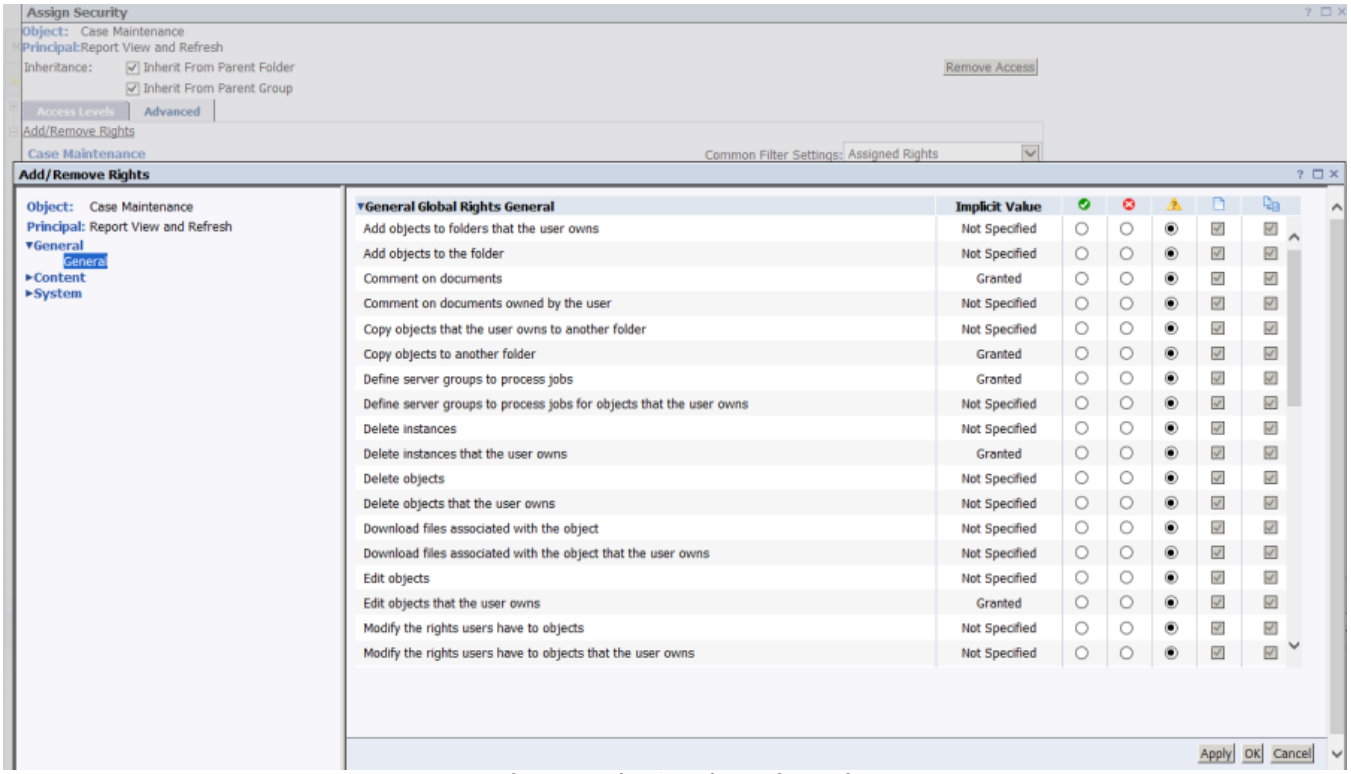


Figure – Assign Security – Advanced

Expand "Content" and click on "Crystal Reports" section. These rights should also be set based on the security group

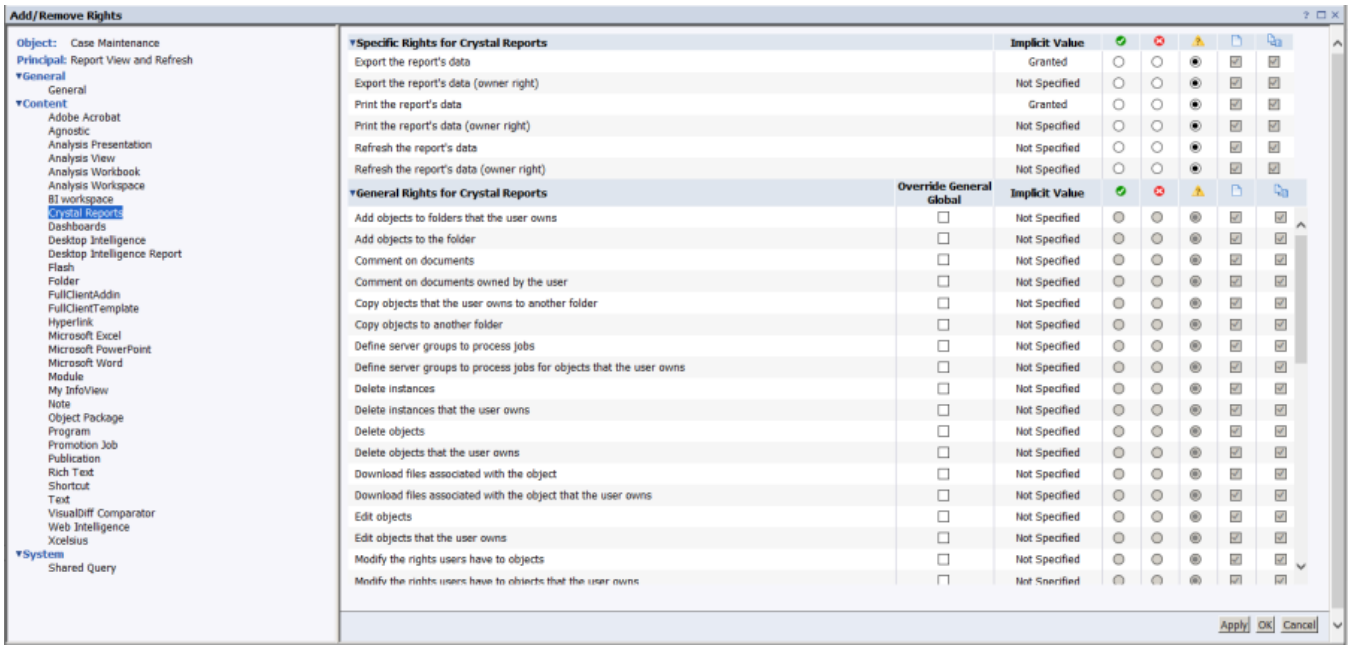


Figure – Advanced Rights – Crystal Reports Section

Hyperlinks/Functions

The following hyperlink functionality is associated with the Advanced Rights screen – Report section:

Hyperlink	Function
Apply	Saves and applies but stays on same screen.
OK	Saves and applies changes and returns to previous screen.
Cancel	Returns to previous page.

Data Elements

None

DSD 6/Architecture – System Security/Business Processes /Screen Designs/BusinessObjects Screens/Add Principals – Adding a New Security Group

CI	Document Name
CI-67057 - DSD SC Add Principals Adding a New Security Group IMPLEMENTED	DSD_SC_Add_Principals_Adding_a_New_Security_Group.doc

From the User Security, click "Add Principals", highlight the groups you want to add, click the "**>**" button and then click "Add and Assign Security". Later add the "Access Levels" and click "Ok".

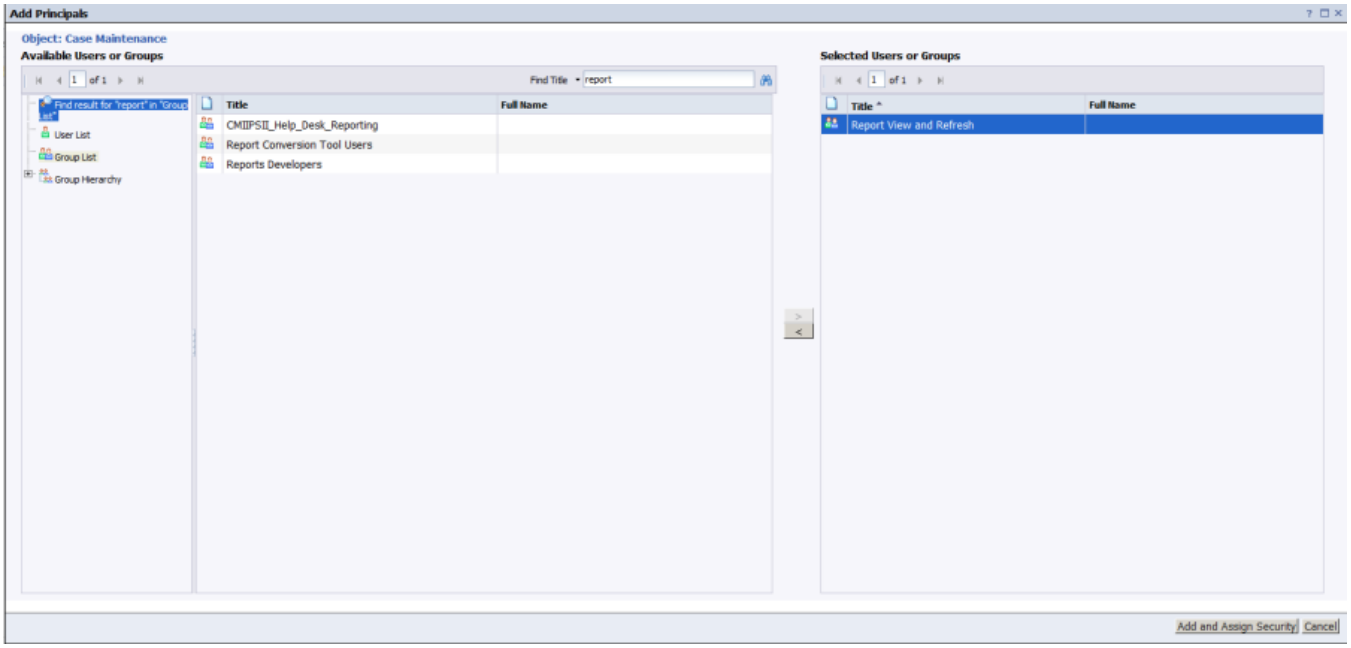


Figure – Add Principals– Adding a New Security Group

Hyperlinks/Functions

The following hyperlink functionality is associated with the Add Principals screen:

Hyperlink	Function
Add and Assign Security	Adds the Group and navigates to "Assign Security" screen
Cancel	Returns to previous page.

Data Elements

None

DSD 6/Architecture – System Security/Business Processes /Screen Designs/BusinessObjects Screens/Report Properties

CI	Document Name
CI-67065 - DSD SC Report Properties IMPLEMENTED	DSD_SC_Report_Properties.doc

Select any report from a folder, right-click on the report and click on "Properties" to show the general properties of that report.

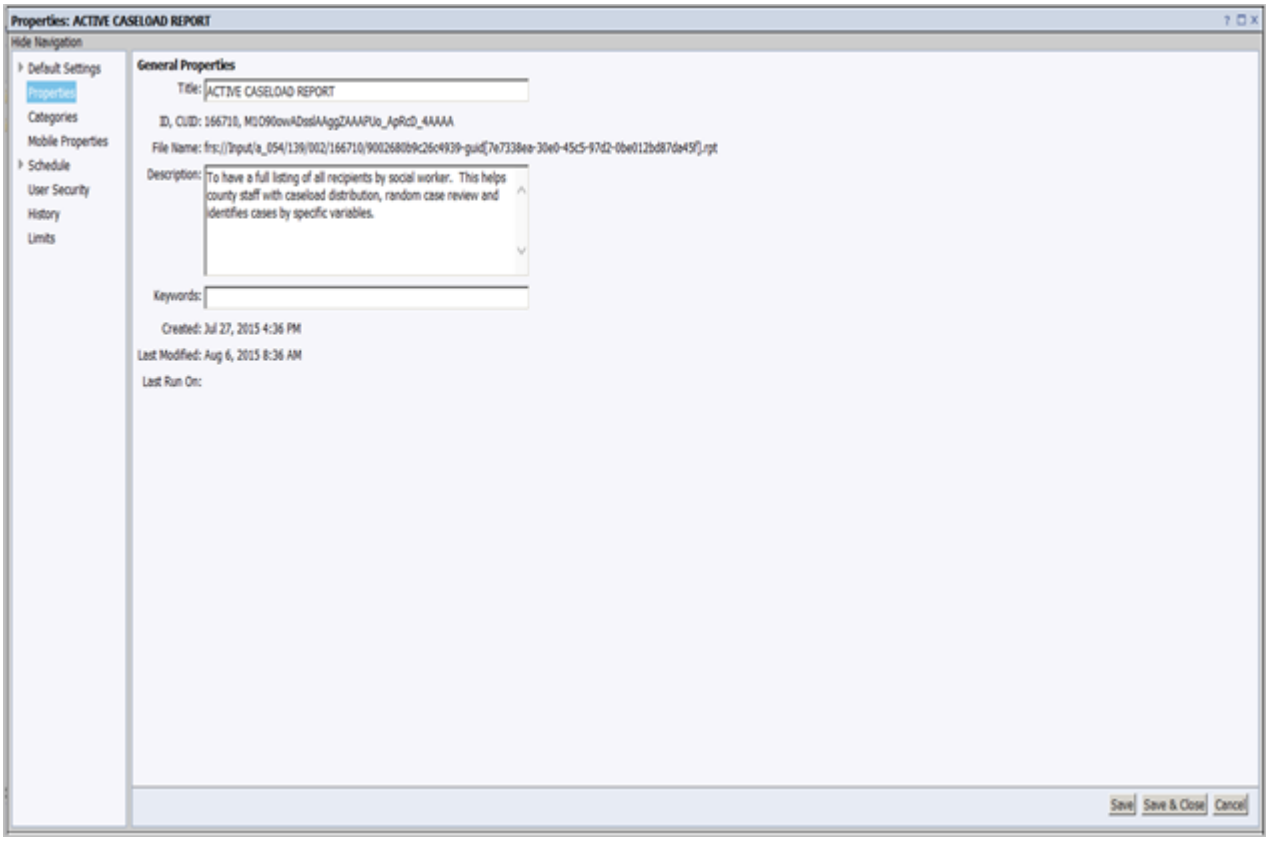


Figure – Report Properties

Hyperlinks/Functions

The following hyperlink functionality is associated with the Report Properties:

Hyperlink	Function
Save	Saves changes to the properties and stays on same screen
Save & Close	Saves changes to the properties and returns to previous page
Cancel	Returns to previous page

Data Elements

The following data elements are specific to the Report Properties:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
Title	Provides the title of report	Text	No	No	Yes
Description	Provides a description of the report	Text	No	No	Yes
Keyword	Provides the key words for searching for report	Text	No	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/CMIPS II Web Portal Home – Log On (Unsecure)

CI	Document Name
CI-67071 - DSD SC CMIPS II Dynamic Web Portal Log On IMPLEMENTED	DSD_SC_CMIPS_II_Dynamic_Web_Portal_Log_On.doc

This is the initial screen displayed upon accessing the CMIPS II Web Portal.

Figure – Log On

Hyperlinks/Functions

The following hyperlink functionality is associated with the Web Portal Log On Screen:

Hyperlink	Function
<CMIPS II Logo>	Opens the CommsHub Home screen as a separate window.
Help	Opens the CMIPS Online Help system as a separate window.
CommsHub	Opens the CommsHub Home screen as a separate window.
Log On	Verifies the user's password and display the Web Portal Secure Home Page for this user upon successful login. **Note:** If this is the user's first time logging in, this button will instead display the Enter New Password and Verify screen.

Data Elements

The following data elements are specific to the Web Portal Log On screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User ID	CMIPS assigned User ID	String	Yes	No	Yes
Password	CMIPS Password (case sensitive)	String	Yes	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Reset Password – CMIPS II

CI	Document Name
CI-67068 - DSD SC Reset Password CMIPS II IMPLEMENTED	DSD_SC_Reset_Password_CMIPS_II.doc

This screen displays when the user selects the Reset Password link on the left navigation of the unsecure Web Portal.

Figure – Reset Password – CMIPS II

Hyperlinks/Functions

The following hyperlink functionality is associated with the Reset Password screen:

Hyperlink	Function
Get Challenge Questions	Randomly selects one of the user's challenge questions and displays Challenge Questions screen

Data Elements

The following data elements are specific to the Reset Password screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User ID	CMIPS-assigned User ID	String	Yes	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Challenge Question

CI	Document Name
CI-67046 - DSD SC Challenge Question IMPLEMENTED	DSD_SC_Challenge_Question.doc

This screen displays when the user has selected Get Challenge Questions from the Reset Password screen. This screen will initially display a single randomly selected challenge question to be answered. If the user fails to answer this question correctly, then the remaining two challenge questions display.

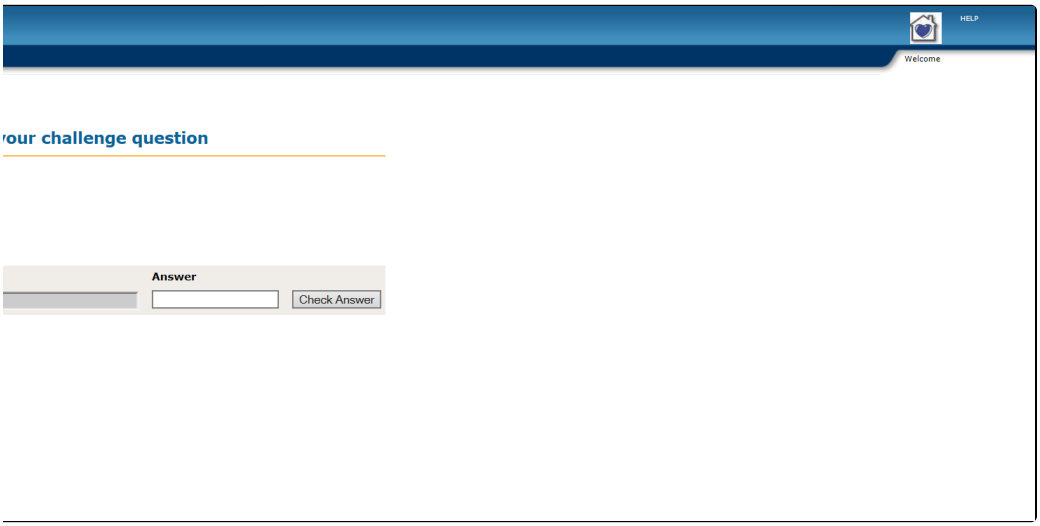


Figure – Challenge Question

Hyperlinks/Functions

The following hyperlink functionality is associated with the Challenge Question screen:

Hyperlink	Function
Check Answer	Compares inputted answer for an identical match to saved answer

Data Elements

The following data elements are specific to the Challenge Question screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User Id	Displays the user's ID	String	No	No	No
Challenge Question	Displays the randomly selected challenge question.	String	No	No	No
Answer	Input associated answer to challenge question. If the user fails to match the first challenge question, the user must match both of the remaining challenge questions letter for letter. The answer is case sensitive.	String	Yes	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Update User Profile

CI	Document Name
CI-67053 - DSD SC Update User Profile IMPLEMENTED	DSD_SC_Update_User_Profile.doc

The user profile is used by the Security Officer or Administrator to manage the user's account. If the user is in a county then only the associated County Security Officer, County Security Administrator, the State Security Officer or the CGI CMIPS Security Officer can manage the security profile of that individual user. If the user is a state user then State Security Officer or the CGI CMIPS Security Officer can manage the security profile of that individual user. This screen displays when a user selects the Update Profile link from the User List screen.

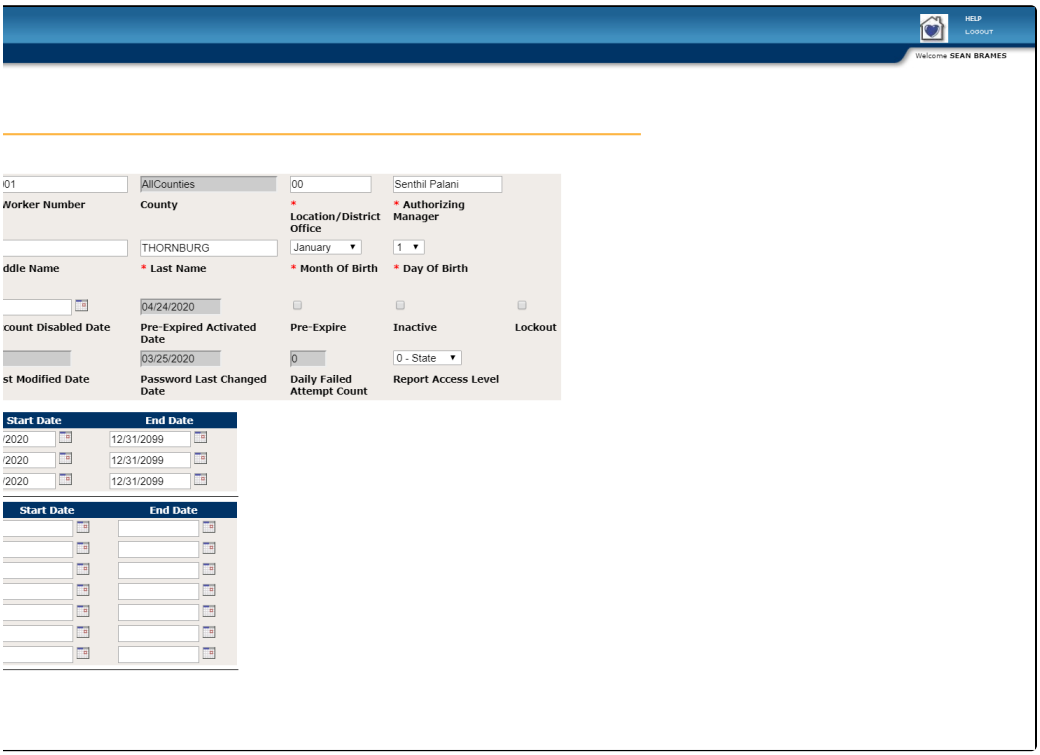


Figure – Update User Profile

Hyperlinks/Functions

The following hyperlink functionality is associated with the Update User Profile screen:

Hyperlink	Function
Update	Updates the user's profile.

Data Elements

The following data elements are specific to the User Profile screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User ID	The User ID associated with record.	String	No	No	No
Worker Number	The user's worker number.	String	Yes	No	Yes

County	The user's county name.	String	No	No	No
Location/District Office	The district office ID. Must be numeric two digits.	Integer	Yes	No	Yes
Authorizing Manager	The person who signed the user account form.	String	Yes	No	Yes
First Name	The user's first name.	String	Yes	No	Yes
Middle Name	The user's middle name.	String	No	No	Yes
Last Name	The user's last name.	String	Yes	No	Yes
Month of Birth	The month of user's birth.	Drop-down list	Yes	No	Yes
Day of Birth	The day of user's birth	Drop-down list	Yes	No	Yes
Account Effective Date	The date the user will have access to the Web portal. Only the Security Officer can activate an account.	Date (MM/DD /YYYY)	No	No	Yes
Account Disabled Date	The date the user will have access denied to the Web portal.	Date (MM/DD /YYYY)	No	No	Yes
Pre-expired Activated Date	The system generated date that the user must change their password or be locked out.	Date (MM/DD /YYYY)	No	No	No
Pre-Expire	Indicates if the current password is required to be changed in the next 30 days or the account will be locked out.	Checkbox	No	No	Yes
Inactive	Indicates if the account has been inactivated due to invalid response to challenge questions or inactivity for 90 days.	Checkbox	No	No	Yes
Lockout	Indicates the account is locked out.	Checkbox	No	No	Yes
Last Logon Date	The date of the last successful logon.	Date (MM/DD /YYYY)	No	No	No
Last Modified Date	The date of the last modification to the user's security profile.	Date (MM/DD /YYYY)	No	no	No
Password Last Changed Date	The date of the last change to the password.	Date (MM/DD /YYYY)	No	No	No
Daily Failed Attempt Count	The number of failed attempts.	Integer	No	No	No
Report Access Level	Indicates the view access level for a user in BusinessObjects Reporting: 0 – State 1 - County 2 - Worker	Drop-down list	No	No	Yes
Web Portal Start Date	The date that access to Web Portal starts.	Date (MM/DD /YYYY)	Yes	No	Yes
Web Portal End Date	The date that access to Web Portal is denied.	Date (MM/DD /YYYY)	Yes	No	Yes
Case Management Start Date	The date that access to Cúram Case Management starts.	Date (MM/DD /YYYY)	No	No	Yes
Case Management End Date	The date that access to Cúram Case Management is denied.	Date (MM/DD /YYYY)	No	No	Yes
Report Access Start Date	The date that access to BusinessObjects Reporting starts.	Date (MM/DD /YYYY)	No	No	Yes
Report Access End Date	The date that access to BusinessObjects Reporting is denied.	Date (MM/DD /YYYY)	No	No	Yes
Portal Role(s) 1 to 7	Portal security role(s).	Drop-down list	No	No	Yes
Start Date	Start date for the Portal Role.	Date (MM/DD /YYYY)	No	No	Yes
End Date	End date for the Portal Role.	Date (MM/DD /YYYY)	No	No	Yes
Password	Security Officer/Administrator's password to confirm changes to user's security profile.	String	Yes	No	Yes – Encrypted

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Enter New Password

CI
CI-67049 - DSD SC Enter New Pwd IMPLEMENTED

The following screen displays when a user has successfully answered the challenge question(s) for a password reset from the unsecure Web Portal or has selected Reset Password from within the secure Web Portal.

Figure – Enter New Password

Hyperlinks/Functions

The following hyperlink functionality is associated with the Enter New Password screen:

Hyperlink	Function
Submit	Updates the user's password.

Data Elements

The following data elements are specific to the Enter New Password screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
New Password	Enter password.	String	Yes	No	Yes
Verify Password	Enter same password for verification.	String	Yes	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Maintain Account Information

CI	Document Name
CI-67066 - DSD SC Maintain Account Information IMPLEMENTED	DSD_SC_Maintain_Account_Information.doc

The screen displays the user's own account information and challenge questions. This screen is accessed from Maintain Account on the left navigation.

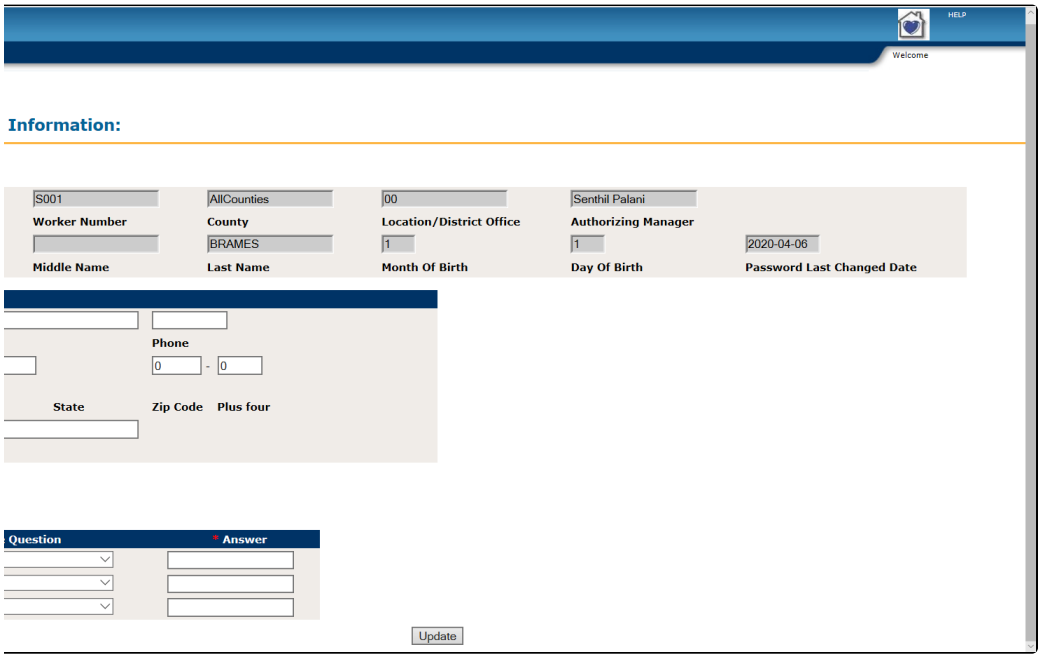


Figure – Maintain Account Information

Hyperlinks/Functions

The following hyperlink functionality is associated with the Maintain Account Information screen:

Hyperlink	Function
Update	Updates the user information database row based on the User ID entered

Data Elements

The following data elements are specific to the Maintain Account Information screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User Id	The User ID associated with record	String	No	No	No
Worker Number	The end user's worker number assigned by the county	String	No	No	No
County	The end user's county name	String	No	No	No
Location/District Office	May be used by the Security Officer to identify the location of the user	Number	No	No	No

Authorizing Manager	The person who signed the user account form	String	No	No	No
First Name	The user's first name	String	No	No	No
Middle Name	The user's middle name	String	No	No	No
Last Name	The users last name	String	No	No	No
Month of Birth	The month of user's birth (M)	Integer	No	No	No
Day of Birth	The day of user's birth (D)	Integer	No	No	No
Password Last Change Date	The date the user last changed their password – good for 60 days	Date (YYYY-MM-DD)	No	No	No
Office Mailing Address					
Street Address	The user's office street address	String	No	No	Yes
Phone	The user's office phone number including area code.	Number	No	No	Yes
City	The user's office city address	String	No	No	Yes
State	The user's office state = CA	String	No	No	No
ZIP Code	The user's ZIP code	Number	No	No	Yes
Plus four	The user's +four ZIP code	Number	No	No	Yes
Email	The user's office email	String	No	No	Yes
Password					
Password	User's password (required to commit updates)	String	Yes	No	Yes – encrypted
Challenge Questions					
Challenge Question 1	User-selected challenge question	Drop down list	Yes	No	Yes
Answer Question 1	User-entered challenge question answer	String	Yes	No	Yes
Challenge Question 2	User-selected challenge question	Drop down list	Yes	No	Yes
Answer Question 2	User-entered challenge question answer	String	Yes	No	Yes
Challenge Question 3	User-selected challenge question	Drop down list	Yes	No	Yes
Answer Question 3	User-entered challenge question answer	String	Yes	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Security Administration Home Page

CI	Document Name
CI-67075 - DSD SC Security Administration Home Page IMPLEMENTED	DSD_SC_Security_Administration_Home_Page.doc

This is the home page for Security Administration. This page displays when the user selects the link for Security Administration from the left navigation.

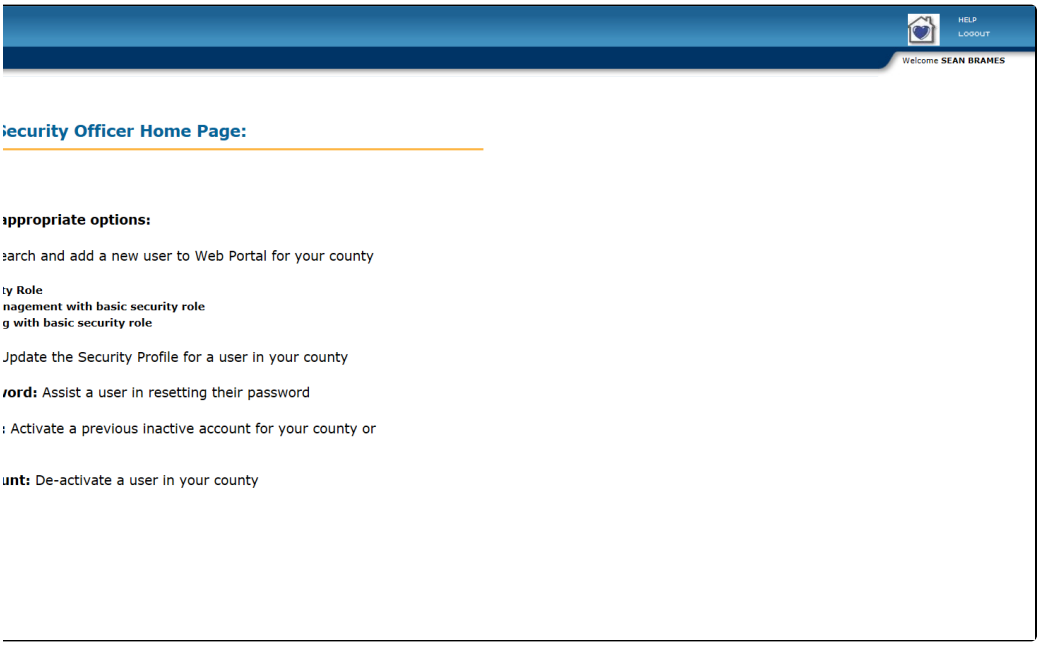


Figure – Security Administration Home Page

Hyperlinks/Functions

There is no hyperlink functionality associated with the Security Administration Home Screen.

Data Elements

There are no data elements specific to the Security Administration Home Page screen.

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Search Active User

CI	Document Name
CI-67069 - DSD SC Search Active User IMPLEMENTED	DSD_SC_Search_Active_User.doc

Basic search screen used by the Security Officer, Security Administrator and the CMIPS Help Desk to find a user and navigate to the User Profile, Activate User or Deactivate User. A County Security Officer or Administrator only sees their county's users. This search screen displays when the User selects the link for Security Profile, Reset User Password, Activate Account or Deactivate Account from the left navigation.

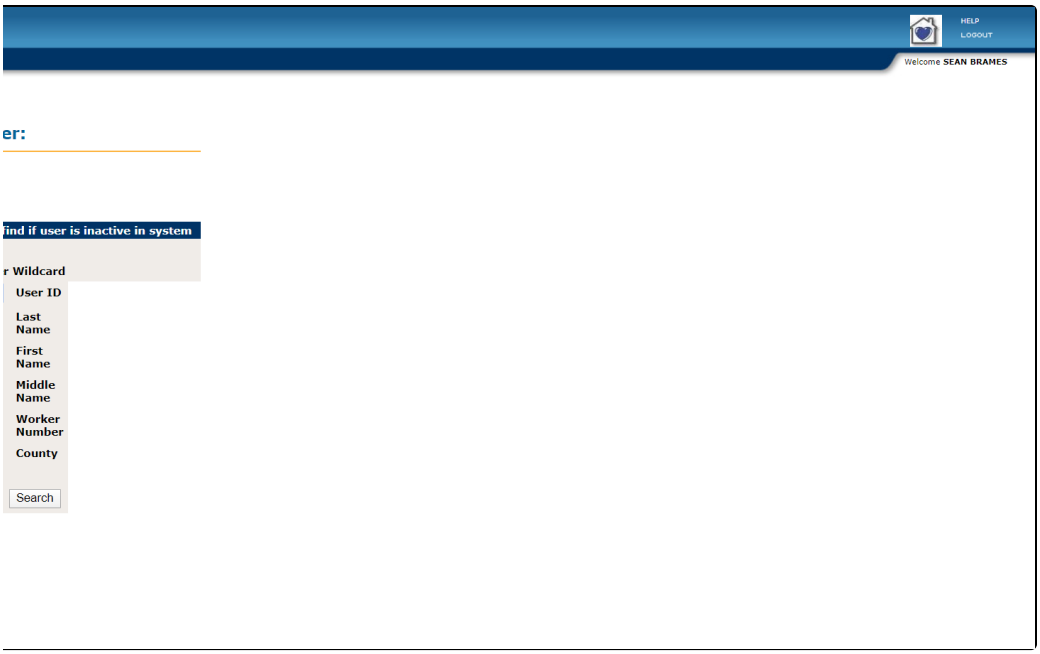


Figure – Search Active User

Hyperlinks/Functions

The following hyperlink functionality is associated with the Search End User screen:

Hyperlink	Function
Search	Search for the user based upon data provided and display the Search Results screen.

Data Elements

The following data elements are specific to the Search Active User screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User ID	Enter user's ID.	String	No	No	Yes
Last Name	Enter user's last name.	String	No	No	Yes
First Name	Enter user's first name.	String	No	No	Yes

Middle Name	Enter user's middle name.	String	No	No	Yes
Worker Number	Enter user's county worker number.	String	No	No	Yes
County	Select user's county name. The County Security Officer/Administrator will only be able to choose his/her own county.	Drop-down list	No	Yes – User's County from security profile	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Search User

CI	Document Name
CI-67073 - DSD SC Search User New IMPLEMENTED	DSD_SC_Search_User_New.doc

The following screen is a unique screen used by a Security Officer to verify that the new user to be added is not already in the CMIP system prior to adding. It is understood that in special cases an individual may have multiple user IDs for two or more counties when a unique security profile is required for the work done in each individual county. This search screen displays when the User selects the link for Add New User from the left navigation.

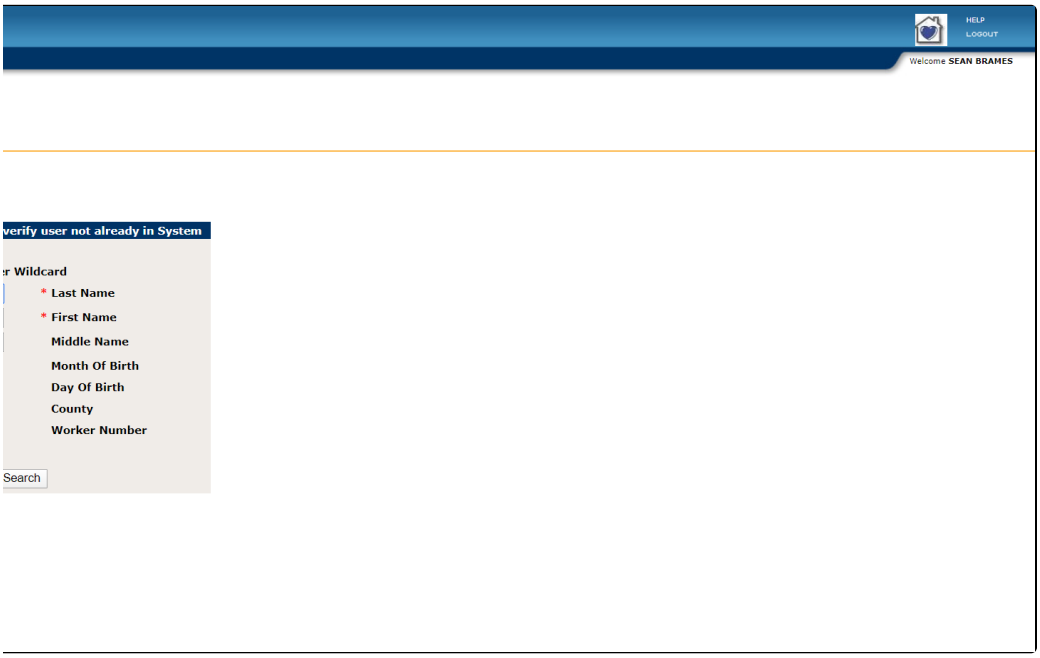


Figure – Search User

Hyperlinks/Functions

The following hyperlink functionality is associated with the Search User screen:

Hyperlink	Function
Search	Search for the user based upon data provided and displays the User List screen

Data Elements

The following data elements are specific to the Search User screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
Last Name	Enter user's last name	Text	Yes (at least one letter)	No	Yes
First Name	Enter user's first name	Text	Yes (at least one letter)	No	Yes
Middle Name	Enter user's middle name	Text	Yes	No	Yes
Month of Birth	Enter user's month of birth (Month's full name)	Drop-down list	No	No	Yes

Day of Birth	Enter user's day of birth (DD)	Drop-down list	No	No	Yes
County	Select user's county name. County Security Officer/Administrator will only be able to choose his/her own county.	Drop-down list	No	Yes – User's county from security profile	Yes
Worker Number	The county's assigned worker number	String	No	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Search Results

CI	Document Name
CI-67077 - DSD SC Search Results IMPLEMENTED	DSD_SC_Search_Results.doc

This Search Results screen displays the results based upon the criteria entered on the Search User screen.

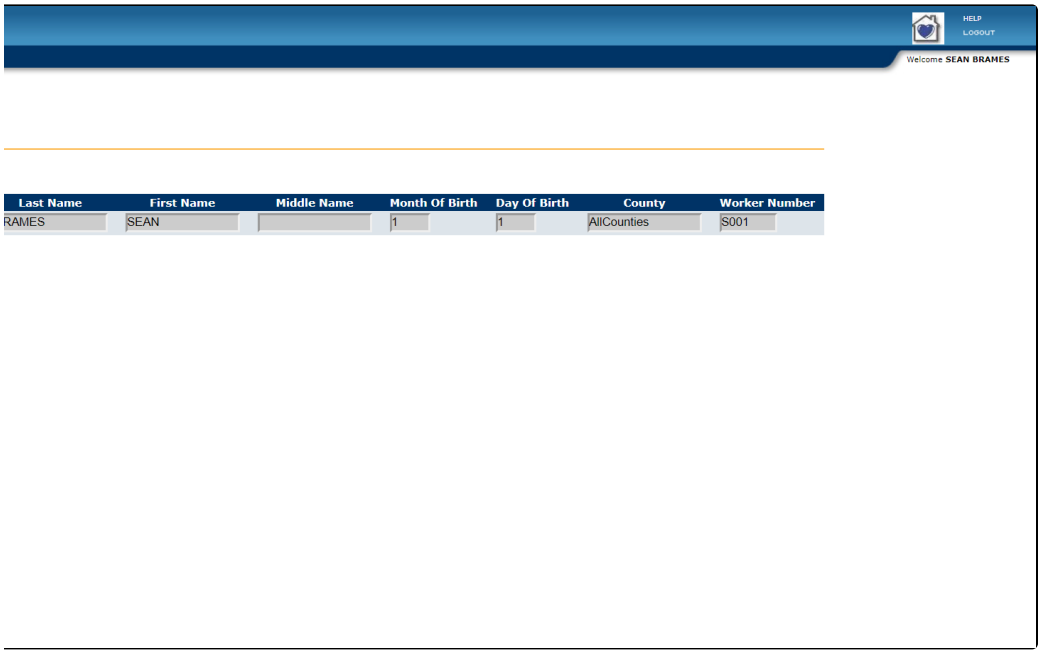


Figure – Search Results

Hyperlinks/Functions

The following hyperlink functionality is associated with the Search Results screen:

Hyperlink	Function
Previous	Displays the prior page of users (button is gray if not applicable)
Next	Displays the next page of users (button is gray if not applicable)
Create User (if from Add New User link)	Displays the Create User screen
Update Profile (if from Security Profile link)	Displays the Update User Profile screen
Verify User (if from Reset User Password)	Displays the Verify User screen
Deactivate (if from Deactivate Account)	Displays the Deactivate User screen
Activate (if from Activate Account)	Displays the Update User Profile screen

Data Elements

The following data elements are specific to the Search Results screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User ID	User's logon ID	String	No	No	No

Last Name	User's last name	String	No	No	No
First Name	User's first name	String	No	No	No
Middle Name	User's middle name	String	No	No	No
Month of Birth	User's month of birth (MM) – only displays when searching to Add a New User	Integer	No	No	No
Day of Birth	User's day of birth (DD) – only displays when searching to Add a New User	Integer	No	No	No
County	County user's county name	String	No	No	No
Worker Number	User's county-assigned worker number	String	No	No	No

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Verify User

CI	Document Name
CI-67070 - DSD SC Verify User IMPLEMENTED	DSD_SC_Verify_User.doc

The below screen is used by the Security Administrator or the CGI CMIPS Help Desk to verify the identity of the user prior to resetting the user's password. Displays when the user selects Verify User from the Search Results screen for Reset User Password.

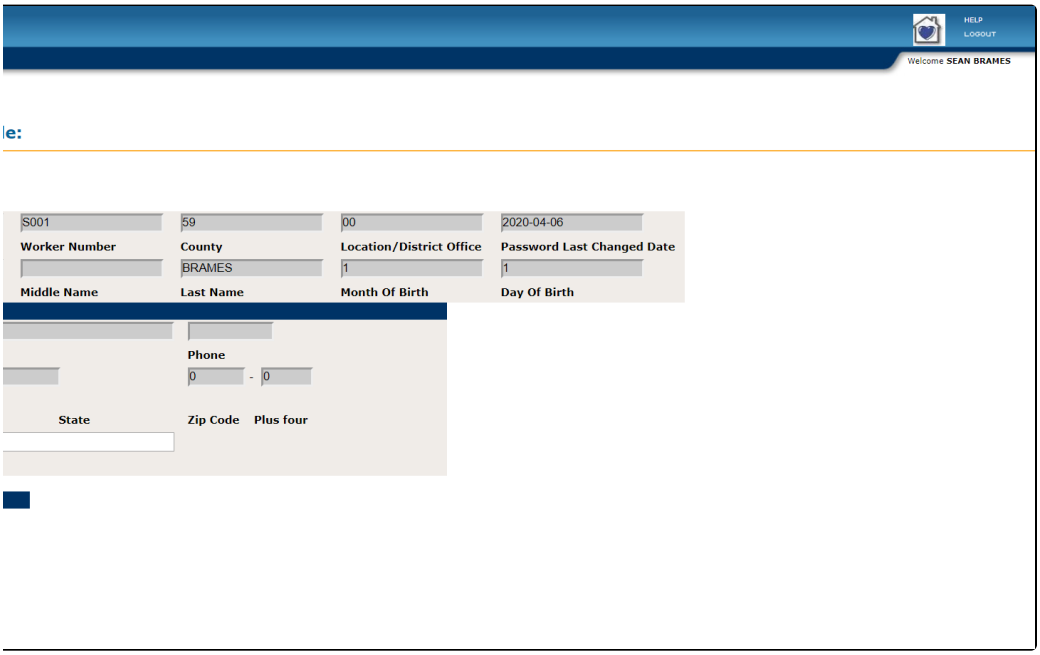


Figure – Verify User

Hyperlinks/Functions

The following hyperlink functionality is associated with the Verify User screen:

Hyperlink	Function
Confirm	Allows the user to verify the user information and precede to the user's challenge questions

Data Elements

The following data elements are specific to the Verify User screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User Id	The User ID for the selected user	String	No	No	No
Worker Number	The end-user's worker number assigned by the county	String	No	No	No
County	The end user's associated county code	Integer	No	No	No
Location/District Office	The district office ID	Number	No	No	No
Password Last Changed Date	The date the user first changed his/her password – good for 60 days	Date (YYYY-MM-DD)	No	No	No
First Name	The user's first name	String	No	No	No
Middle Name	The user's middle name	String	No	No	No

Last Name	The user's last name	String	No	No	No
Month of Birth	The month of user's birth (M)	Integer	No	No	Yes
Day of Birth	The day of user's birth (D)	Integer	No	No	Yes
Office Mailing Address					
Street Address	The user's office street address	String	No	No	No
Phone	The user's office phone number including area code	Number	No	No	No
City	The user's office city address	String	No	No	No
State	The user's office state = CA	String	No	No	No
ZIP Code	The user's ZIP code	Number	No	No	No
Plus Four	The user's +four ZIP code	Number	No	No	No
Email	The user's office email	String	No	No	No
Password					
Password	Password of the Security Officer/Administrator	String	Yes	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/System Assigned Password

CI
CI-67060 - DSD SC System Assigned Pwd IMPLEMENTED

The below screen is used to inform the Security Officer, Security Administrator, or the CMIPS Help Desk of the new system-assigned password. This is the only time the pre-expired password is shown in a non-encrypted format for communication to the user. At first login within 30 days the user is prompted to update their password, challenge questions and user administrative information. Displays when the user successfully answers challenge questions for resetting a user's password by the Security Officer/Administrator.

Figure – System Assigned Password

Hyperlinks/Functions

The following hyperlink functionality is associated with the System Assigned Password screen:

Hyperlink	Function
Confirm	Allows the user to confirm the new password assignment.

Data Elements

The following data elements are specific to the System Assigned Password screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User ID	User ID	String	No	No	No
Password	System-generated password (only time the password will be displayed for communication to end-user).	String	No	No	No
Password Expire Date	The date the system-generated password will expire.	Date (MM/DD /YYYY)	No	No	No

Your Password	Password of the Security Officer, Security Administrator or Help Desk staff who has changed the password.	String	Yes	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Create User

CI	Document Name
CI-67052 - DSD SC Create User IMPLEMENTED	DSD_SC_Create_User.doc

This screen is used by the Security Officer to establish the account and access of a new user of the CMIPS system. This screen displays when Create User is selected from the User List screen. Only the Security Officer is authorized to create a new User.

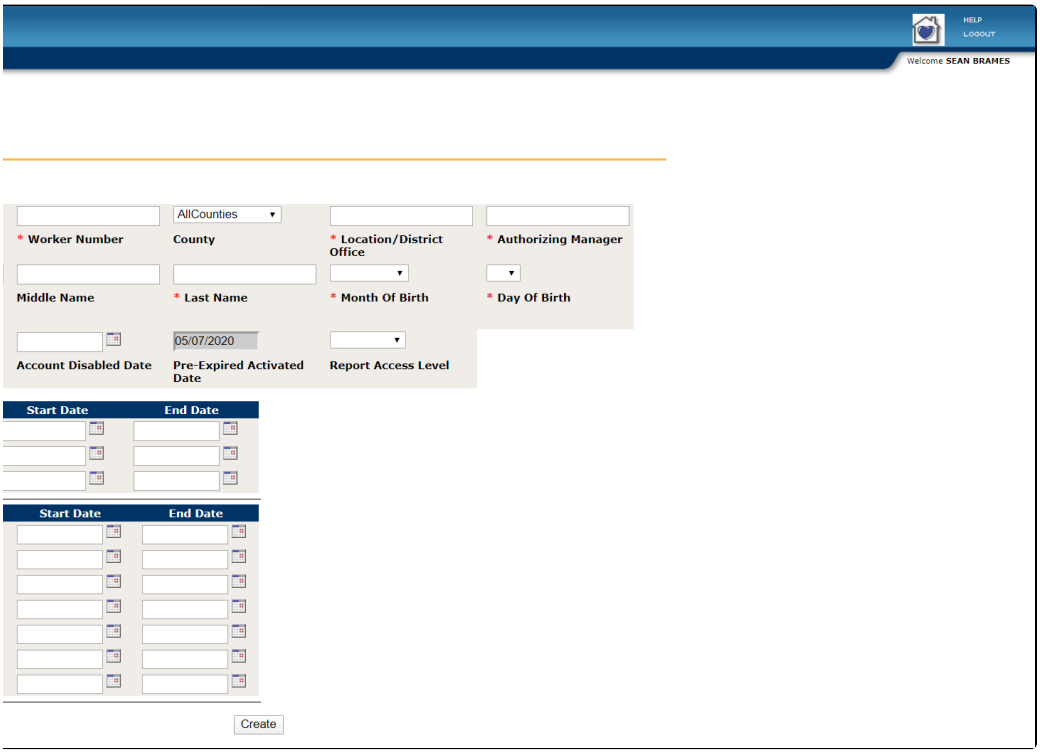


Figure – Create User

Hyperlinks/Functions

The following hyperlink functionality is associated with the Create User screen:

Hyperlink	Function
Create	Creates the user and displays the system assigned password.

Data Elements

The following data elements are specific to the Create User screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User Id	The User ID associated with record.	String	Yes	No	Yes
Worker Number	The end user's worker number assigned by the county.	String	Yes	No	Yes
County	The end user's county code name.	Drop-down list	No	Defaulted to the Security. Officer /Administrator's County	Yes

Location/ District Office	The district office ID (must be numeric two digits).	Number	Yes	No	Yes
Authorizing Manager	The person who signed the user account form.	String	Yes	No	Yes
First Name	The user's first name.	String	Yes	No	Yes
Middle Name	The user's middle name.	String	No	No	Yes
Last Name	The user's last name.	String	Yes	No	Yes
Month of Birth	The month of user's birth (Month's full name).	Drop-down list	Yes	No	Yes
Day of Birth	The day of user's birth (D).	Drop-down list	Yes	No	Yes
Account Effective Date	The date the user was created or activated.	Date (MM/DD /YYYY)	No	Today's Date	No
Account Disabled Date	The date the user is deactivated.	Date (MM/DD /YYYY)	No	No	Yes
Pre-expired Activated Date	The system-generated date that the user must change password or be locked out.	Date (MM/DD /YYYY)	No	Yes. System-generated 30 days from account creation.	No
Report Access Level	Indicates the access level for a user within BusinessObjects.	Drop-down list	No	No	Yes
Web Portal Start Date	The date that access to Web Portal starts.	Date (MM/DD /YYYY)	Yes	No	Yes
Web Portal End Date	The date that access to Web Portal is denied.	Date (MM/DD /YYYY)	Yes	No	Yes
Case Management Start Date	The date that access to Cúram Case Management starts.	Date (MM/DD /YYYY)	No	No	Yes
Case Management End Date	The date that access to Cúram Case Management is denied.	Date (MM/DD /YYYY)	No	No	Yes
Report Access Start Date	The date that access to BusinessObjects Reporting starts.	Date (MM/DD /YYYY)	No	No	Yes
Report Access End Date	The date that access to BusinessObjects Reporting is denied.	Date (MM/DD /YYYY)	No	No	Yes
Portal Role(s) 1 to 7	Portal security role(s).	Drop down list	No	No	Yes
Start Date	Start Portal Roles.	Date (MM/DD /YYYY)	No	No	Yes
End Date	End Portal Roles.	Date (MM/DD /YYYY)	No	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/End User ID and System Assigned Password

CI
CI-67054 - DSD SC End User ID and System Assigned Pwd IMPLEMENTED

The following screen provides the Security Officer with the assigned user ID, new pre-expired password and the status of the Case Management and BusinessObjects user ID creation.

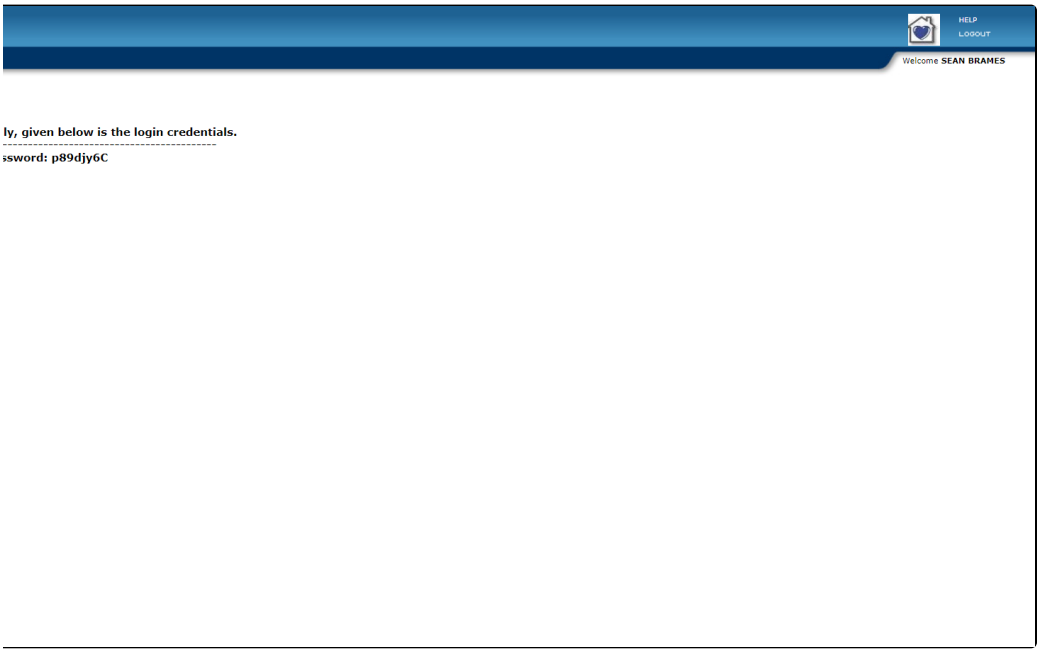


Figure – End-User ID and System Assigned Password

Hyperlinks/Functions

There are no hyperlinks associated with the End User ID and System Assigned Password screen.

Data Elements

The following data elements are specific to the End User ID and System Assigned Password screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User ID	User ID	String	No	No	No
Password	System-generated password (only time the password will be displayed for communication to end user).	String	No	No	No
Web Portal	Status of user ID creation in Web Portal.	String	No	No	No
Case Management	Status of user ID creation in Case Management. **Note:** Only displays if a Case Management start and end date were entered on the Create User screen.	String	No	No	No
Reporting	Status of user ID creation in BusinessObjects Reporting. **Note:** Only displays if a Reporting start and end date were entered on the Create User screen.	String	No	No	No

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Deactivate Account

CI	Document Name
CI-67062 - DSD SC Deactivate Account IMPLEMENTED	DSD_SC_Deactivate_Account.doc

The following screen is the confirmation of the deactivation of an account that requires the Security Officer or Security Administrator to successfully enter his or her password prior to the commitment of the deactivation of an account. The screen displays when the security officer/administrator has selected Deactivate Account from the left navigation and selected deactivate for a user from the Search Results screen.

Figure – Deactivate Account

Hyperlinks/Functions

The following hyperlink functionality is associated with the Deactivate Account screen:

Hyperlink	Function
Confirm	Confirms the deactivation of the account.

Data Elements

The following data elements are specific to the Deactivate Account screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User ID	User ID to be deactivated.	String	No	No	No
Password	Password of the Security Officer/Administrator.	String	Yes	No	Yes

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Portal Security Screens/Navigation Elements

The following Navigational Links are displayed in the left navigation menu for the Cases Menu (the plus sign indicates it is based on the security role and the indent signifies the expansion once it is selected):

Left Navigation Menu	Description	User Role
CMIPS II Web Portal Home (Non-Secure)	Displays CMIPS Web Portal Home screen prior to Logon	All Users
Log On	Displays CMIPS Logon screen	All Users
Reset Password	Displays the Reset Password screen	All Users
General Help	Displays General Help screen	All Users
CMIPS II Web Portal Home (Secure)	Displays CMIPS Web Portal Home screen	All Users
Reset Password	Displays Reset Password screen	All Users
Maintain Account	Displays User Account Information screen	All Users
+ Case Management	Displays screen with Link to Case Management if web Portal Security Profile allows	Must have Case Management access
+ Reporting	Displays screen with Link to BusinessObjects Reports if web Portal Security Profile allows	Must have Reporting access
+ Advantage HRM (payroll)	Displays screen with Link to CGI Advantage HRM if web Portal Security Profile allows	Must have Advantage HRM (payroll) access
+ Advantage Financial	Displays screen with Link to CGI Advantage Financial if web Portal Security Profile allows	Must have Advantage Financial access
+ CMIPS II Query and Sampling Tool	Displays CMIPS Query and Sampling Tool Home if Web Portal Security Profile allows	Must have Query and Sampling access
+ Reports	Displays CMIPS Query and Sampling Tool Reports screen	Must have Query and Sampling access
+ Criteria	Displays CMIPS Query screen	Must have Query and Sampling access
+ Form SOC293	Displays CMIPS Form SOC293 Query screen	Must have Query and Sampling access
+ Form SOC426	Displays CMIPS Form SOC426 Query screen	Must have Query and Sampling access
+ Sampling	Displays CMIPS Sampling screen	Must have Query and Sampling access
+ Tasks	Displays CMIPS Tasks screen	Must have Query and Sampling access
+ Security Administration	Displays Web Portal Security Administration screen if web Portal Security Profile allows	Must have Security Officer or Security Administrator access
+ Add New User	Displays Web Portal Security Administration Add User screen if web Portal Security Profile allows	Must have Security Officer access
+ Security Profile	Displays Web Portal Security Administration Assign User Roles screen if web Portal Security Profile allows	Must have Security Officer or Security Administrator access
+ Reset User Password	Displays Web Portal Security Administration Reset User Password screen if web Portal Security Profile allows	Must have Security Officer or Security Administrator access
+ Activate Account	Displays screen to select users currently deactivated which may be selected for activation.	Must have Security Officer access

+ Deactivate Account	Displays screen to select active users which may be selected for deactivation.	Must have Security officer or Security Administrator access
+ Report Security	Displays Business Objects Central Management Console (CMC) to allow the Security Officer or Administrator to set up users in Business Objects	Must have Security officer or Security Administrator access
+ Data Retention	Displays Retention Home screen if Web Portal Security Profile allows	Must have Data Retention access
+ Suspend	Displays Suspend from Logical Delete and Purge screen if Web Portal Security Profile allows	Must have Data Retention access
+ Restore	Displays Move record from Logical Delete to Active screen if Web Portal Security Profile allows	Must have Data Retention access
Help	Displays Help	All Users
CMIPS II Notifications	Displays any Notification screen from the CMIPS Help Desk	All Users
CMIPS II Contacts	Displays CMIPS Contact screen	All Users
+ Web Portal Content	Displays screen for maintain Web content for the Web Master	Must have Web Master access
+TPF Manager	Displays screen to capture metrics for TPF	TPF Manager
+TPF Metrics Collection	Displays screen to capture metrics for TPF	TPF Manager
+TPF Metrics Modify	Displays screen to modify metrics for TPF	TPF Manager

Note: The "+" indicates a specific user security profile is needed to view these navigation bar options.

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Advantage Screens

DSD 6/Architecture – System Security/Business Processes /Screen Designs/Advantage Screens/Advantage Login Screen

CI	Document Name
CI-116568 - DSD SC Advantage Login Screen IMPLEMENTED	DSD_SC_Advantage_Login_Screen.doc

This is the initial screen displayed upon accessing the Advantage application:

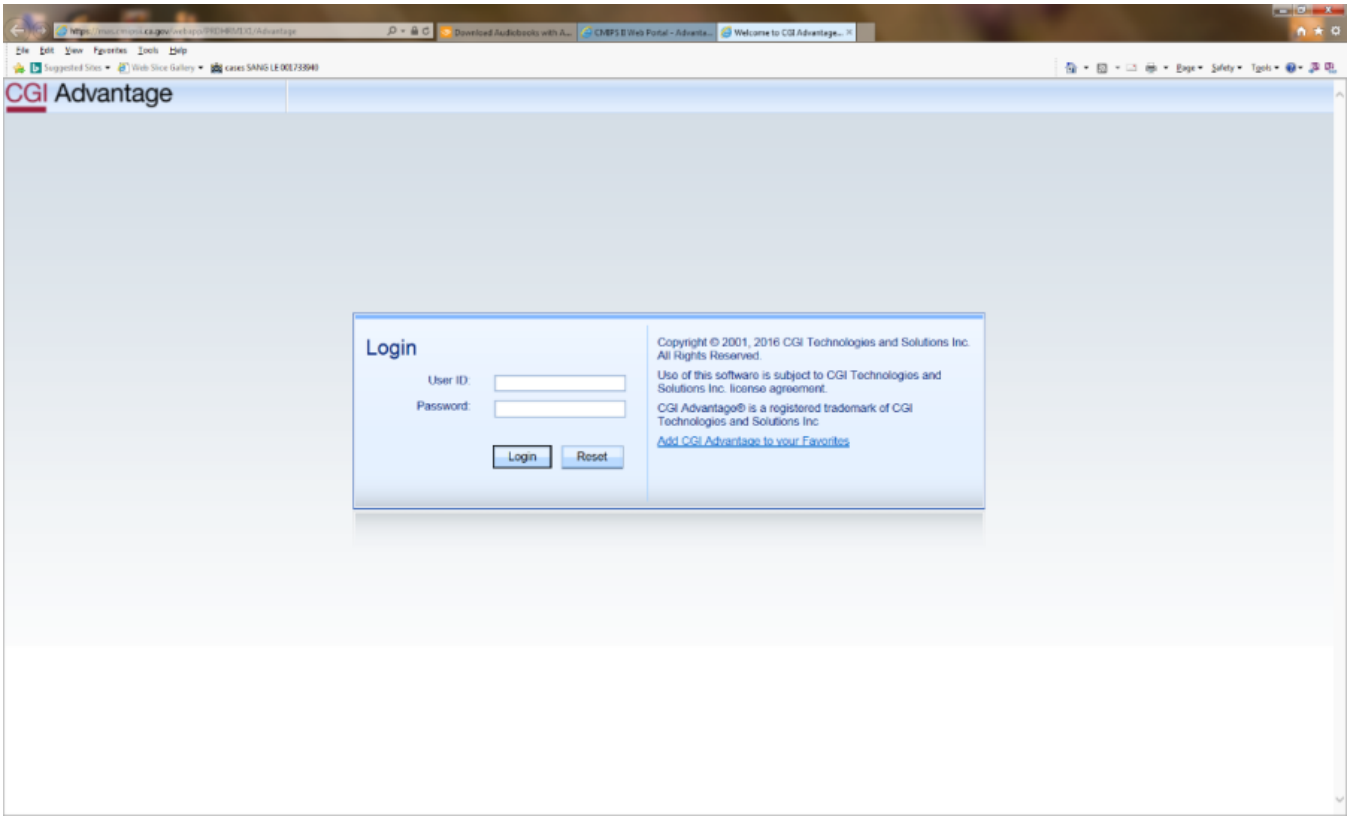


Figure – Advantage Login

Hyperlinks/Functions

The following hyperlink functionality is associated with the Advantage Login Screen.

Hyperlink	Function
Login	Authenticate user
Reset	Clear the Login/password text

Data Elements

The following data elements are specific to the Advantage Login screen:

Field Name	Help	Data Type	Required Indicator	Default Value	Editable Field
User ID	CMIPS assigned User ID	String	Yes	No	Yes

Password	CMIPS password (case sensitive)	String	Yes	No	Yes

DSD 6/Architecture – System Security/Business Processes /Error Messages

This section will define the validation edits on the CMIPS Dynamic Web Portal screens and will document the error messages that will be displayed for each edit.

No	Requirement ID	CI	Screen Name or User Action	Condition	Action	Error
1	12745	CI-110996 - DSD EM SS 01 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID and/or password do not match CMIPS security profile for the user on the initial entry	Do not allow the action	The following message appears on the screen: "2 of 3 attempts. User ID and Password did not match."
2	12745	CI-110997 - DSD EM SS 02 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID and/or password do not match CMIPS security profile for the user on the second entry	Do not allow the action	The following message appears on the screen: "3 of 3 attempts. Final attempt prior to lock out. User ID and Password did not match."
3	12745	CI-110998 - DSD EM SS 03 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID and/or password do not match CMIPS security profile for the user on the third entry	Do not allow the action. Lock the user's security access.	The following message appears on the screen: "Your account is locked. Please contact your Security Administrator to unlock your account."
4	12758	CI-110999 - DSD EM SS 04 IMPLEMENTED	Reset Password – CMIPS II Web Portal	User ID entered is not found within CMIPS	Do not allow the action.	The following message appears on the screen: "ID Does Not Exist. Please Contact Help Desk."
5	12779	CI-111000 - DSD EM SS 05 IMPLEMENTED	Challenge Question – CMIPS II Web Portal	The answer for the first challenge question does not match the answer previously provided according to the user's security profile	Do not allow the action	The following message appears on the screen: "Answer did not match. Try the next two."
6	12779	CI-111001 - DSD EM SS 06 IMPLEMENTED	Challenge Question – CMIPS II Web Portal	The answers to the remaining two challenge questions do not match the answers previously provided according to the user's security profile	Do not allow the action. Lock the User's security access.	The following message appears on the screen: "Your answers did not match. Your account is locked. Please contact your Security Administrator to unlock your account."
7	12752	CI-111002 - DSD EM SS 07 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Password matches one of the most recent 10 passwords for this user	Do not allow the action.	The following message appears on the screen: "Password must not match one of your most recent 10 passwords."
8	12735	CI-111003 - DSD EM SS 08 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Password is fewer than eight characters in length	Do not allow the action	The following message appears on the screen: "Password must be at least 8 characters in length."
9	12735	CI-111004 - DSD EM SS 09 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Password does not contain three of the following four character types: English upper-case characters (A-Z) English lower-case characters (a-z) Base 10 digits (0-9) Non-alphanumeric (such as !,$, #, %)	Do not allow the action	The following message appears on the screen: "Passwords did not match or did not meet the criteria"
10	12748	CI-111005 - DSD EM SS 10 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Password has already been reset today	Do not allow the action	The following message appears on the screen: "Password has already been reset today."

11	12748	CI-111006 - DSD EM SS 11 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Verify Password does not match the New Password	Do not allow the action	The following message appears on the screen: "Passwords did not match".
12		Cancelled				
13	12756	CI-111008 - DSD EM SS 13 IMPLEMENTED	Search User (Add New User) – CMIPS II Web Portal	Day of birth is not a valid day for the indicated month of birth	Do not allow the action	The following message appears on the screen: "The Day of Birth must be a day within the indicated month."
14	12756	CI-111009 - DSD EM SS 14 IMPLEMENTED	Search User (Add New User) – CMIPS II Web Portal	Worker number is not four characters in length	Do not allow the action	The following message appears on the screen: "Worker Number must be four characters in length."
15	12756	CI-111010 - DSD EM SS 15 IMPLEMENTED	Search User (Add New User) – CMIPS II Web Portal	County code selected does not match the county code of the logged in user and the logged in User is not associated with "All Counties"	Do not allow the action	The following message appears on the screen: "You are only authorized to search Users within your county."
16	12756	CI-111011 - DSD EM SS 16 IMPLEMENTED	Create User – CMIPS II Web Portal	User name already exists within the CMIPS system	Do not allow the action	The following message appears on the screen: "User ID already exists. Please update to be a unique User ID".
17	12756	CI-111012 - DSD EM SS 17 IMPLEMENTED	Create User – CMIPS II Web Portal	Worker number is not four characters in length	Do not allow the action	The following message appears on the screen: "Worker Number must be four characters in length."
18		Cancelled				
19	12756	CI-111014 - DSD EM SS 19 IMPLEMENTED	Create User – CMIPS II Web Portal	Day of birth is not a valid day for the indicated month of birth	Do not allow the action	The following message appears on the screen: "The Day of Birth must be a day within the indicated month."
20	12730	CI-111015 - DSD EM SS 20 IMPLEMENTED	Create User – CMIPS II Web Portal	Case Management Start date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Case Management Start Date must not be before the Account Effective Date".

No	Requirement ID	CI	Screen Name or User Action	Condition	Action	Error
21	12756	CI-111016 - DSD EM SS 21 IMPLEMENTED	Create User – CMIPS II Web Portal	Account Disabled Date falls between the Case Management Start and Case Management End Dates	Do not allow the action	The following message appears on the screen: "Account is disabled during the Case Management access period".
22	12756	CI-111017 - DSD EM SS 22 IMPLEMENTED	Create User – CMIPS II Web Portal	Case Management End date is prior to Case Management Start date	Do not allow the action	The following message appears on the screen: "Case Management End Date cannot be before Case Management Start Date."
23	12756	CI-111018 - DSD EM SS 23 IMPLEMENTED	Create User – CMIPS II Web Portal	Report Start date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Report Start Date must not be before the Account Effective Date".
24	12730	CI-111019 - DSD EM SS 24 IMPLEMENTED	Create User – CMIPS II Web Portal	Account Disabled Date falls between the Report Start and Report End Dates	Do not allow the action	The following message appears on the screen: "Account is disabled during the Report access period".
25	12756	CI-111020 - DSD EM SS 25 IMPLEMENTED	Create User – CMIPS II Web Portal	Report End date is prior to Reports Start date	Do not allow the action	The following message appears on the screen: "Reports End Date cannot be before Reports Start Date."
26	12756	CI-111021 - DSD EM SS 26 IMPLEMENTED	Create User – CMIPS II Web Portal	Web Portal Start date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Web Portal Start Date must not be before the Account Effective Date".

27	12756	CI-111022 - DSD EM SS 27 IMPLEMENTED	Create User – CMIPS II Web Portal	Account Disabled Date falls between the Web Portal Start and Web Portal End Dates	Do not allow the action	The following message appears on the screen: "Account is disabled during the Web Portal access period."
28	12756	CI-111023 - DSD EM SS 28 IMPLEMENTED	Create User – CMIPS II Web Portal	Web Portal End date is prior to Web Portal Start Date	Do not allow the action	The following message appears on the screen: "Web Portal End Date cannot be before Web Portal Start Date."
29	12756	CI-111024 - DSD EM SS 29 IMPLEMENTED	Create User – CMIPS II Web Portal	Portal Role Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Portal Role Start Date must not be before the Web Portal Start Date".
30	12756	CI-111025 - DSD EM SS 30 IMPLEMENTED	Create User – CMIPS II Web Portal	Web Portal End Date falls between the Portal Role Start and Portal Role End Dates	Do not allow the action	The following message appears on the screen: "Web Portal access ends during the Portal Role access period".
31	12756	CI-111026 - DSD EM SS 31 IMPLEMENTED	Create Use – CMIPS II Dynamic Web Portal r	Portal Role End date is prior to Portal Role Start date	Do not allow the action	The following message appears on the screen: "Portal Role End Date cannot be before Portal Role Start Date."
32	12756	CI-111027 - DSD EM SS 32 IMPLEMENTED	Create User – CMIPS II Web Portal	The same Portal Role is selected more than once from the Portal Role drop down list	Do not allow the action	The following message appears on the screen: "Portal Roses cannot be the same. Please select different roles."
32a	12756	CI-111028 - DSD EM SS 32a IMPLEMENTED	Create User – CMIPS II Web Portal	County Security Officer is assigning a Portal Role of Security Officer or Web Portal Master	Do not allow the action	The following message appears on the screen: "County Security Officer is not authorized to assign the Portal Role of Security Officer or Web Master."
33	12756	CI-111029 - DSD EM SS 33 IMPLEMENTED	Create User – CMIPS II Web Portal	Portal Role is selected and no Start Date is indicated	Do not allow the action	The following message appears on the screen: "Portal Roles Start Date cannot be blank. Please select a value."
34	12664	CI-111030 - DSD EM SS 34 IMPLEMENTED	Search End User – CMIPS II Web Portal	Worker Number is not four characters in length	Do not allow the action	The following message appears on the screen: "Worker Number must be four characters in length."
35		Cancelled				
36	12755 12756	CI-111032 - DSD EM SS 36 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Worker Number is not four characters in length	Do not allow the action	The following message appears on the screen: "Worker Number must be four characters in length."
37	12755 12756	CI-111033 - DSD EM SS 37 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Day of Birth is not a valid day for the indicated Month of Birth	Do not allow the action	The following message appears on the screen: "The Day of Birth must be a day within the indicated month."
38	12755 12756	CI-111034 - DSD EM SS 38 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Case Management Start Date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Case Management Start date must not be before the Account Effective Date."
39	12755 12756	CI-111035 - DSD EM SS 39 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Case Management Start Date is after the Account Disabled Date	Do not allow the action	The following message appears on the screen: "Case Management Start Date must not be after the Account Disabled Date".
40	12755 12756	CI-111036 - DSD EM SS 40 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Case Management End Date is prior to Case Management Start Date	Do not allow the action	The following message appears on the screen: "Case Management End Date cannot be before Case Management Start Date."

No	Requirement ID	CI	Screen Name or User Action	Condition	Action	Error

41	12755 12756	CI-111037 - DSD EM SS 41 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Report Start Date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Report Start date must not be before the Account Effective Date."
42	12755 12756	CI-111038 - DSD EM SS 42 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Report Start Date is after the Account Disabled Date	Do not allow the action	The following message appears on the screen: "Report Start Date must not be after the Account Disabled Date."
43	12755 12756	CI-111039 - DSD EM SS 43 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Report End date is prior to Report Start date	Do not allow the action	The following message appears on the screen: "Report End Date cannot be before Reports Start Date."
44	12755 12756	CI-111040 - DSD EM SS 44 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Web Portal Start Date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Web Portal Start Date must not be before the Account Effective Date."
45	12756	CI-111041 - DSD EM SS 45 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Web Portal Start Date is after the Account Disabled Date	Do not allow the action	The following message appears on the screen: "Web Portal Start Date must not be after the Account Disabled Date."
46	12755 12756	CI-111042 - DSD EM SS 46 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Web Portal End Date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Web Portal End date cannot be before Web Portal Start Date."
47	12755 12756	CI-111043 - DSD EM SS 47 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Portal Role Start Date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Portal Role Start Date must not be before the Web Portal Start Date."
48	12755 12756	CI-111044 - DSD EM SS 48 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Portal Role End date is prior to Portal Role Start date	Do not allow the action	The following message appears on the screen: "Portal Role End Date cannot be before Portal Role Start Date."
49	12755 12756	CI-111045 - DSD EM SS 49 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	The same Portal Role is selected more than once from the Portal Role drop down list	Do not allow the action	The following message appears on the screen: "Portal Roles cannot be Same. Please select different Roles."
50	12748	CI-111046 - DSD EM SS 50 IMPLEMENTED	Maintain Account – CMIPS II Web Portal	The same Challenge Question is selected more than once from the Challenge Question drop down list	Do not allow the action	The following message appears on the screen: "Each Challenge Question may only be selected once."
51	12756	CI-111047 - DSD EM SS 51 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	If any required field is blank	Do not allow the action	The following message appears on the screen: "XXXX cannot be blank." Where XXXX is the name of the required field.
52	12755 12756	CI-111048 - DSD EM SS 52 IMPLEMENTED	Create User – CMIPS II Web Portal	Portal Role is selected and no Start Date is indicated	Do not allow the action	The following message appears on the screen: "Portal Roles Start Date cannot be blank. Please select a value."
53	12755 12756	CI-111049 - DSD EM SS 53 IMPLEMENTED	Create User – CMIPS II Web Portal	Portal Role is not selected and Start Date or End Date is indicated	Do not allow the action	The following message appears on the screen: "Please Select the Portal Role. Date is populated"
54	12755 12756	CI-111050 - DSD EM SS 54 IMPLEMENTED	Update User Profile	Portal Role is not selected and Start Date or End Date is indicated	Do not allow the action	The following message appears on the screen: "Please Select the Portal Role. Date is populated"
55	12755 12756	CI-111051 - DSD EM SS 55 IMPLEMENTED	Create User – CMIPS II Web Portal	Case Management Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Case Management Start Date must not be before the Web Portal Start Date."
56	12755 12756	CI-111052 - DSD EM SS 56 IMPLEMENTED	Create User – CMIPS II Web Portal	Reports Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Report Start Date must not be before the Web Portal Start Date."
57	12755 12756	CI-111053 - DSD EM SS 57 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Case Management Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Case Management Start Date must not be before the Web Portal Start Date."

58	12726 12758 12756	CI-111054 - DSD EM SS 58 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Reports Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Report Start Date must not be before the Web Portal Start Date."
59	12758 12726	CI-111055 - DSD EM SS 59 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID is locked	Do not allow the action.	The following message appears on the screen: "Your account is locked. Please contact your Security Administrator to unlock your account."
60	12726 12758	CI-111056 - DSD EM SS 60 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID does not exist	Do not allow the action	The following message appears on the screen: "User ID does not exist."

No	Requirement ID	CI	Screen Name or User Action	Condition	Action	Error
61	12758	CI-111057 - DSD EM SS 61 IMPLEMENTED	Verify User (from Reset Password for User) – CMIPS II Web Portal	Upon selecting confirm and the User Account is Inactivated	Do not allow the action	The following message appears on the screen: "This account is marked inactive, use the "Activate Account" procedure instead. If you are a Security Administrator, you are required to have a Security Officer perform this action."
62	12755 12756	CI-111058 - DSD EM SS 62 IMPLEMENTED	Create User – CMIPS II Web Portal	When the logon user is "All Counties" and the user is trying to create a user in one county and he/she selected one or more of the following security roles: AdvantageHRM AdvantageFinancial WebMasterUsers TPFManager	Do not allow the action	The following message appears on the screen: "Selected Role is invalid for a County User."
63	12756 12758	CI-111059 - DSD EM SS 63 IMPLEMENTED	Challenge Question – CMIPS II Web Portal	When the logon user is the Security Officer or Security Administrator and the attempt to answer the user's challenge questions fails	Do not allow the action.	The following message appears on the screen: "The selected user account has been Inactivated. Contact your Security Officer to Activate this account."
64	12755 12756	CI-111060 - DSD EM SS 64 IMPLEMENTED	Create User – CMIPS II Web Portal	If the user has selected the following two Web Portal Roles: Security Officer Security Administrator	Do not allow the action	The following message appears on the screen: "A user may not have the role of Security Officer and Security Administrator."
65	12755 12756	CI-111061 - DSD EM SS 65 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	If the user has selected the following two Web Portal Roles: Security Officer Security Administrator	Do not allow the action	The following message appears on the screen: "A user may not have the role of Security Officer and Security Administrator."
66	12755 12756	CI-111062 - DSD EM SS 66 IMPLEMENTED	Create User – CMIPS II Web Portal	If the user has selected Report Access for a user and has not indicated the Report Access Level	Do not allow the action	The following message appears on the screen: "Report Access Level is required when Report Access is indicated."
67	12755 12756	CI-111063 - DSD EM SS 67 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	If the user has selected Report Access for a user and has not indicated the Report Access Level	Do not allow the action	The following message appears on the screen: "Report Access Level is required when Report Access is indicated."
68	12755 12756	CI-111064 - DSD EM SS 68 IMPLEMENTED	Create User – CMIPS II Web Portal	If the user has selected Report Access Level of "0 – State" and the user is not indicated as "All Counties"	Do not allow the action	The following message appears on the screen: "Report Access Level not allowed for a County user."
69	12755 12756	CI-111065 - DSD EM SS 69 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	If the user has selected Report Access Level of "0 – State" and the user is not indicated as "All Counties"	Do not allow the action	The following message appears on the screen: "Report Access Level not allowed for a County user."
70	12758 12756	CI-111066 - DSD EM SS 70 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID is inactivated	Do not allow the action	The following message appears on the screen: "The selected user account has been Inactivated. Contact your Security Officer to Activate this account."

71	12756	CI-111067 - DSD EM SS 71 IMPLEMENTED	Create User – CMIPS II Web Portal	Location/District Office is not two digits numeric	Do not allow the action	The following message appears on the screen: "Please enter a valid District Office Code."
72	12756	CI-111068 - DSD EM SS 72 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Location/District Office is not two digits numeric	Do not allow the action	The following message appears on the screen: "Please enter a valid District Office Code."
73	12343 12356	CI-674822 - DSD EM SS 73 IMPLEMENTED	Create User – CMIPS II Web Portal	The two digit District Office number is other than "00" and does not match an existing District Office in the indicated County	Do not allow the action	Display the error message "The District Office is not valid for indicated County."
74	12343 12356	CI-674823 - DSD EM SS 74 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	The two digit District Office number is other than "00" and does not match an existing District Office in the indicated County	Do not allow the action	Display the error message "The District Office is not valid for indicated County."

DSD 6/Architecture – System Security/Business Processes /Error Messages (1-20)

This section will define the validation edits on the CMIPS Dynamic Web Portal screens and will document the error messages that will be displayed for each edit.

No	Requirement ID	CI	Screen Name or User Action	Condition	Action	Error
1	12745	CI-110996 - DSD EM SS 01 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID and/or password do not match CMIPS security profile for the user on the initial entry	Do not allow the action	The following message appears on the screen: "2 of 3 attempts. User ID and Password did not match."
2	12745	CI-110997 - DSD EM SS 02 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID and/or password do not match CMIPS security profile for the user on the second entry	Do not allow the action	The following message appears on the screen: "3 of 3 attempts. Final attempt prior to lock out. User ID and Password did not match."
3	12745	CI-110998 - DSD EM SS 03 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID and/or password do not match CMIPS security profile for the user on the third entry	Do not allow the action. Lock the user's security access.	The following message appears on the screen: "Your account is locked. Please contact your Security Administrator to unlock your account."
4	12758	CI-110999 - DSD EM SS 04 IMPLEMENTED	Reset Password – CMIPS II Web Portal	User ID entered is not found within CMIPS	Do not allow the action.	The following message appears on the screen: "ID Does Not Exist. Please Contact Help Desk."
5	12779	CI-111000 - DSD EM SS 05 IMPLEMENTED	Challenge Question – CMIPS II Web Portal	The answer for the first challenge question does not match the answer previously provided according to the user's security profile	Do not allow the action	The following message appears on the screen: "Answer did not match. Try the next two."
6	12779	CI-111001 - DSD EM SS 06 IMPLEMENTED	Challenge Question – CMIPS II Web Portal	The answers to the remaining two challenge questions do not match the answers previously provided according to the user's security profile	Do not allow the action. Lock the User's security access.	The following message appears on the screen: "Your answers did not match. Your account is locked. Please contact your Security Administrator to unlock your account."
7	12752	CI-111002 - DSD EM SS 07 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Password matches one of the most recent 10 passwords for this user	Do not allow the action.	The following message appears on the screen: "Password must not match one of your most recent 10 passwords."
8	12735	CI-111003 - DSD EM SS 08 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Password is fewer than eight characters in length	Do not allow the action	The following message appears on the screen: "Password must be at least 8 characters in length."
9	12735	CI-111004 - DSD EM SS 09 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Password does not contain three of the following four character types: English upper-case characters (A-Z) English lower-case characters (a-z) Base 10 digits (0-9) Non-alphanumeric (such as !,$, #, %)	Do not allow the action	The following message appears on the screen: "Passwords did not match or did not meet the criteria"
10	12748	CI-111005 - DSD EM SS 10 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Password has already been reset today	Do not allow the action	The following message appears on the screen: "Password has already been reset today."
11	12748	CI-111006 - DSD EM SS 11 IMPLEMENTED	Enter New Password – CMIPS II Web Portal	Verify Password does not match the New Password	Do not allow the action	The following message appears on the screen: "Passwords did not match".
12		Cancelled				

13	12756	CI-111008 - DSD EM SS 13 IMPLEMENTED	Search User (Add New User) – CMIPS II Web Portal	Day of birth is not a valid day for the indicated month of birth	Do not allow the action	The following message appears on the screen: "The Day of Birth must be a day within the indicated month."
14	12756	CI-111009 - DSD EM SS 14 IMPLEMENTED	Search User (Add New User) – CMIPS II Web Portal	Worker number is not four characters in length	Do not allow the action	The following message appears on the screen: "Worker Number must be four characters in length."
15	12756	CI-111010 - DSD EM SS 15 IMPLEMENTED	Search User (Add New User) – CMIPS II Web Portal	County code selected does not match the county code of the logged in user and the logged in User is not associated with "All Counties"	Do not allow the action	The following message appears on the screen: "You are only authorized to search Users within your county."
16	12756	CI-111011 - DSD EM SS 16 IMPLEMENTED	Create User – CMIPS II Web Portal	User name already exists within the CMIPS system	Do not allow the action	The following message appears on the screen: "User ID already exists. Please update to be a unique User ID".
17	12756	CI-111012 - DSD EM SS 17 IMPLEMENTED	Create User – CMIPS II Web Portal	Worker number is not four characters in length	Do not allow the action	The following message appears on the screen: "Worker Number must be four characters in length."
18		Cancelled				
19	12756	CI-111014 - DSD EM SS 19 IMPLEMENTED	Create User – CMIPS II Web Portal	Day of birth is not a valid day for the indicated month of birth	Do not allow the action	The following message appears on the screen: "The Day of Birth must be a day within the indicated month."
20	12730	CI-111015 - DSD EM SS 20 IMPLEMENTED	Create User – CMIPS II Web Portal	Case Management Start date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Case Management Start Date must not be before the Account Effective Date".

DSD 6/Architecture – System Security/Business Processes /Error Messages (21-40)

No	Requirement ID	CI	Screen Name or User Action	Condition	Action	Error
21	12756	CI-111016 - DSD EM SS 21 IMPLEMENTED	Create User – CMIPS II Web Portal	Account Disabled Date falls between the Case Management Start and Case Management End Dates	Do not allow the action	The following message appears on the screen: "Account is disabled during the Case Management access period".
22	12756	CI-111017 - DSD EM SS 22 IMPLEMENTED	Create User – CMIPS II Web Portal	Case Management End date is prior to Case Management Start date	Do not allow the action	The following message appears on the screen: "Case Management End Date cannot be before Case Management Start Date."
23	12756	CI-111018 - DSD EM SS 23 IMPLEMENTED	Create User – CMIPS II Web Portal	Report Start date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Report Start Date must not be before the Account Effective Date".
24	12730	CI-111019 - DSD EM SS 24 IMPLEMENTED	Create User – CMIPS II Web Portal	Account Disabled Date falls between the Report Start and Report End Dates	Do not allow the action	The following message appears on the screen: "Account is disabled during the Report access period".
25	12756	CI-111020 - DSD EM SS 25 IMPLEMENTED	Create User – CMIPS II Web Portal	Report End date is prior to Reports Start date	Do not allow the action	The following message appears on the screen: "Reports End Date cannot be before Reports Start Date."
26	12756	CI-111021 - DSD EM SS 26 IMPLEMENTED	Create User – CMIPS II Web Portal	Web Portal Start date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Web Portal Start Date must not be before the Account Effective Date".
27	12756	CI-111022 - DSD EM SS 27 IMPLEMENTED	Create User – CMIPS II Web Portal	Account Disabled Date falls between the Web Portal Start and Web Portal End Dates	Do not allow the action	The following message appears on the screen: "Account is disabled during the Web Portal access period."
28	12756	CI-111023 - DSD EM SS 28 IMPLEMENTED	Create User – CMIPS II Web Portal	Web Portal End date is prior to Web Portal Start Date	Do not allow the action	The following message appears on the screen: "Web Portal End Date cannot be before Web Portal Start Date."
29	12756	CI-111024 - DSD EM SS 29 IMPLEMENTED	Create User – CMIPS II Web Portal	Portal Role Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Portal Role Start Date must not be before the Web Portal Start Date".
30	12756	CI-111025 - DSD EM SS 30 IMPLEMENTED	Create User – CMIPS II Web Portal	Web Portal End Date falls between the Portal Role Start and Portal Role End Dates	Do not allow the action	The following message appears on the screen: "Web Portal access ends during the Portal Role access period".
31	12756	CI-111026 - DSD EM SS 31 IMPLEMENTED	Create Use – CMIPS II Dynamic Web Portal r	Portal Role End date is prior to Portal Role Start date	Do not allow the action	The following message appears on the screen: "Portal Role End Date cannot be before Portal Role Start Date."
32	12756	CI-111027 - DSD EM SS 32 IMPLEMENTED	Create User – CMIPS II Web Portal	The same Portal Role is selected more than once from the Portal Role drop down list	Do not allow the action	The following message appears on the screen: "Portal Roses cannot be the same. Please select different roles."
32a	12756	CI-111028 - DSD EM SS 32a IMPLEMENTED	Create User – CMIPS II Web Portal	County Security Officer is assigning a Portal Role of Security Officer or Web Portal Master	Do not allow the action	The following message appears on the screen: "County Security Officer is not authorized to assign the Portal Role of Security Officer or Web Master."
33	12756	CI-111029 - DSD EM SS 33 IMPLEMENTED	Create User – CMIPS II Web Portal	Portal Role is selected and no Start Date is indicated	Do not allow the action	The following message appears on the screen: "Portal Roles Start Date cannot be blank. Please select a value."

34	12664	CI-111030 - DSD EM SS 34 IMPLEMENTED	Search End User – CMIPS II Web Portal	Worker Number is not four characters in length	Do not allow the action	The following message appears on the screen: "Worker Number must be four characters in length."
35		Cancelled				
36	12755 12756	CI-111032 - DSD EM SS 36 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Worker Number is not four characters in length	Do not allow the action	The following message appears on the screen: "Worker Number must be four characters in length."
37	12755 12756	CI-111033 - DSD EM SS 37 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Day of Birth is not a valid day for the indicated Month of Birth	Do not allow the action	The following message appears on the screen: "The Day of Birth must be a day within the indicated month."
38	12755 12756	CI-111034 - DSD EM SS 38 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Case Management Start Date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Case Management Start date must not be before the Account Effective Date."
39	12755 12756	CI-111035 - DSD EM SS 39 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Case Management Start Date is after the Account Disabled Date	Do not allow the action	The following message appears on the screen: "Case Management Start Date must not be after the Account Disabled Date".
40	12755 12756	CI-111036 - DSD EM SS 40 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Case Management End Date is prior to Case Management Start Date	Do not allow the action	The following message appears on the screen: "Case Management End Date cannot be before Case Management Start Date."

DSD 6/Architecture – System Security/Business Processes /Error Messages (41-60)

No	Requirement ID	CI	Screen Name or User Action	Condition	Action	Error
41	12755 12756	CI-111037 - DSD EM SS 41 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Report Start Date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Report Start date must not be before the Account Effective Date."
42	12755 12756	CI-111038 - DSD EM SS 42 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Report Start Date is after the Account Disabled Date	Do not allow the action	The following message appears on the screen: "Report Start Date must not be after the Account Disabled Date."
43	12755 12756	CI-111039 - DSD EM SS 43 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Report End date is prior to Report Start date	Do not allow the action	The following message appears on the screen: "Report End Date cannot be before Reports Start Date."
44	12755 12756	CI-111040 - DSD EM SS 44 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Web Portal Start Date is prior to Account Effective Date	Do not allow the action	The following message appears on the screen: "Web Portal Start Date must not be before the Account Effective Date."
45	12756	CI-111041 - DSD EM SS 45 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Web Portal Start Date is after the Account Disabled Date	Do not allow the action	The following message appears on the screen: "Web Portal Start Date must not be after the Account Disabled Date."
46	12755 12756	CI-111042 - DSD EM SS 46 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Web Portal End Date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Web Portal End date cannot be before Web Portal Start Date."
47	12755 12756	CI-111043 - DSD EM SS 47 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Portal Role Start Date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Portal Role Start Date must not be before the Web Portal Start Date."
48	12755 12756	CI-111044 - DSD EM SS 48 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Portal Role End date is prior to Portal Role Start date	Do not allow the action	The following message appears on the screen: "Portal Role End Date cannot be before Portal Role Start Date."
49	12755 12756	CI-111045 - DSD EM SS 49 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	The same Portal Role is selected more than once from the Portal Role drop down list	Do not allow the action	The following message appears on the screen: "Portal Roles cannot be Same. Please select different Roles."
50	12748	CI-111046 - DSD EM SS 50 IMPLEMENTED	Maintain Account – CMIPS II Web Portal	The same Challenge Question is selected more than once from the Challenge Question drop down list	Do not allow the action	The following message appears on the screen: "Each Challenge Question may only be selected once."
51	12756	CI-111047 - DSD EM SS 51 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	If any required field is blank	Do not allow the action	The following message appears on the screen: "XXXX cannot be blank." Where XXXX is the name of the required field.
52	12755 12756	CI-111048 - DSD EM SS 52 IMPLEMENTED	Create User – CMIPS II Web Portal	Portal Role is selected and no Start Date is indicated	Do not allow the action	The following message appears on the screen: "Portal Roles Start Date cannot be blank. Please select a value."
53	12755 12756	CI-111049 - DSD EM SS 53 IMPLEMENTED	Create User – CMIPS II Web Portal	Portal Role is not selected and Start Date or End Date is indicated	Do not allow the action	The following message appears on the screen: "Please Select the Portal Role. Date is populated"
54	12755 12756	CI-111050 - DSD EM SS 54 IMPLEMENTED	Update User Profile	Portal Role is not selected and Start Date or End Date is indicated	Do not allow the action	The following message appears on the screen: "Please Select the Portal Role. Date is populated"

55	12755 12756	CI-111051 - DSD EM SS 55 IMPLEMENTED	Create User – CMIPS II Web Portal	Case Management Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Case Management Start Date must not be before the Web Portal Start Date."
56	12755 12756	CI-111052 - DSD EM SS 56 IMPLEMENTED	Create User – CMIPS II Web Portal	Reports Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Report Start Date must not be before the Web Portal Start Date."
57	12755 12756	CI-111053 - DSD EM SS 57 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Case Management Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Case Management Start Date must not be before the Web Portal Start Date."
58	12726 12758 12756	CI-111054 - DSD EM SS 58 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Reports Start date is prior to Web Portal Start date	Do not allow the action	The following message appears on the screen: "Report Start Date must not be before the Web Portal Start Date."
59	12758 12726	CI-111055 - DSD EM SS 59 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID is locked	Do not allow the action.	The following message appears on the screen: "Your account is locked. Please contact your Security Administrator to unlock your account."
60	12726 12758	CI-111056 - DSD EM SS 60 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID does not exist	Do not allow the action	The following message appears on the screen: "User ID does not exist."

DSD 6/Architecture – System Security/Business Processes /Error Messages (61-74)

No	Requirement ID	CI	Screen Name or User Action	Condition	Action	Error
61	12758	CI-111057 - DSD EM SS 61 IMPLEMENTED	Verify User (from Reset Password for User) – CMIPS II Web Portal	Upon selecting confirm and the User Account is Inactivated	Do not allow the action	The following message appears on the screen: "This account is marked inactive, use the "Activate Account" procedure instead. If you are a Security Administrator, you are required to have a Security Officer perform this action."
62	12755 12756	CI-111058 - DSD EM SS 62 IMPLEMENTED	Create User – CMIPS II Web Portal	When the logon user is "All Counties" and the user is trying to create a user in one county and he/she selected one or more of the following security roles: AdvantageHRM AdvantageFinancial WebMasterUsers TPFManager	Do not allow the action	The following message appears on the screen: "Selected Role is invalid for a County User."
63	12756 12758	CI-111059 - DSD EM SS 63 IMPLEMENTED	Challenge Question – CMIPS II Web Portal	When the logon user is the Security Officer or Security Administrator and the attempt to answer the user's challenge questions fails	Do not allow the action.	The following message appears on the screen: "The selected user account has been Inactivated. Contact your Security Officer to Activate this account."
64	12755 12756	CI-111060 - DSD EM SS 64 IMPLEMENTED	Create User – CMIPS II Web Portal	If the user has selected the following two Web Portal Roles: Security Officer Security Administrator	Do not allow the action	The following message appears on the screen: "A user may not have the role of Security Officer and Security Administrator."
65	12755 12756	CI-111061 - DSD EM SS 65 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	If the user has selected the following two Web Portal Roles: Security Officer Security Administrator	Do not allow the action	The following message appears on the screen: "A user may not have the role of Security Officer and Security Administrator."
66	12755 12756	CI-111062 - DSD EM SS 66 IMPLEMENTED	Create User – CMIPS II Web Portal	If the user has selected Report Access for a user and has not indicated the Report Access Level	Do not allow the action	The following message appears on the screen: "Report Access Level is required when Report Access is indicated."
67	12755 12756	CI-111063 - DSD EM SS 67 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	If the user has selected Report Access for a user and has not indicated the Report Access Level	Do not allow the action	The following message appears on the screen: "Report Access Level is required when Report Access is indicated."
68	12755 12756	CI-111064 - DSD EM SS 68 IMPLEMENTED	Create User – CMIPS II Web Portal	If the user has selected Report Access Level of "0 – State" and the user is not indicated as "All Counties"	Do not allow the action	The following message appears on the screen: "Report Access Level not allowed for a County user."
69	12755 12756	CI-111065 - DSD EM SS 69 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	If the user has selected Report Access Level of "0 – State" and the user is not indicated as "All Counties"	Do not allow the action	The following message appears on the screen: "Report Access Level not allowed for a County user."
70	12758 12756	CI-111066 - DSD EM SS 70 IMPLEMENTED	CMIPS II Dynamic Web Portal Home	User ID is inactivated	Do not allow the action	The following message appears on the screen: "The selected user account has been Inactivated. Contact your Security Officer to Activate this account."
71	12756	CI-111067 - DSD EM SS 71 IMPLEMENTED	Create User – CMIPS II Web Portal	Location/District Office is not two digits numeric	Do not allow the action	The following message appears on the screen: "Please enter a valid District Office Code."
72	12756	CI-111068 - DSD EM SS 72 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	Location/District Office is not two digits numeric	Do not allow the action	The following message appears on the screen: "Please enter a valid District Office Code."
73	12343 12356	CI-674822 - DSD EM SS 73 IMPLEMENTED	Create User – CMIPS II Web Portal	The two digit District Office number is other than "00" and does not match an existing District Office in the indicated County	Do not allow the action	Display the error message "The District Office is not valid for indicated County."

74	12343 12356	CI-674823 - DSD EM SS 74 IMPLEMENTED	Update User Profile – CMIPS II Web Portal	The two digit District Office number is other than "00" and does not match an existing District Office in the indicated County	Do not allow the action	Display the error message "The District Office is not valid for indicated County."

DSD 6/Architecture – System Security/Business Processes /Error Messages/Security Error Messages for CMIPS II Dynamic Web Portal

DSD 6/Architecture – System Security/Business Processes /Error Messages/Security Error Messages for CMIPS II Dynamic Web Portal (1-10)

This section will define the validation edits on the screens and will document the errors messages that will be displayed for each edit.

No	Requirement ID	CI	Screen Name or User Action	Condition	Action	Error
1	12755 12756	CI-106696 - DSD EM SS WP 01 IMPLEMENTED	Update Profile – CMIPS II Web Portal	Account Effective Date is updated and the User is not designated as a County Security Officer	Do not allow the action	The following message appears on the screen: "User is not authorized to update the Account Effective Date."
2	12755 12756	CI-117820 - DSD EM SS WP 02 IMPLEMENTED	Update Profile – CMIPS II Web Portal	Inactive checkbox is unselected and the User is not designated as a County Security Officer	Do not allow the action	The following message appears on the screen: "User is not authorized to re-activate the account."

DSD 6/Architecture – System Security/Business Processes /Business Rules

DSD 6/Architecture – System Security/Business Processes /Business Rules/CMIPS II User ID Standards Validation and Rules

CI	Document Name
CI-117879 - DSD BR CMIPS II User ID Standards Validation and Rules IMPLEMENTED	DSD_BR_CMIPS_II_User_ID_Standards_Validation_and_Rules.doc

The following CMIPS user ID standards are used to create a user ID:

- Every user name is unique.
- Every user name is traceable to the user.
- User accounts are only disabled and never deleted in Portal, Case Management, BusinessObjects and CGI Advantage.
- Assigned by the Security Administrator
- Concatenation:
- First name Initial
- Last name (seven letters or fewer)
- If required, a three-digit number to make the above combination unique

DSD 6/Architecture – System Security/Business Processes /Business Rules/CMIPS II User Password Standards

CI	Document Name
CI-117878 - DSD BR CMIPS II User Password Standards IMPLEMENTED	DSD_BR_CMIPS_II_User_Password_Standards.doc

Password standards per NIST SP 800-43 and OSI-AP-07-02 are checked and verified with each password reset including those that are system generated. The following are the user password standards:

- Enforce password history: 10 passwords remembered
- Minimum password length: Eight characters
- Passwords must meet complexity requirements and contain characters from three of the following four categories:
- English upper-case characters (A-Z)
- English lower-case characters (a-z)
- Base 10 digits (0-9)
- Non-alphanumeric (!,$, #,%, *, @, ^, and &)
- Passwords expire every 60 days (Service Accounts [non-human] have 365 days or when a CMIPS Operations team member leaves before the CGI expiration period).
- Passwords may only be reset once per day excluding the pre-expired initial change.
- Pre-expired passwords will remain active for 30 days from creation and randomly generated.
- If an account is inactive for 90 days, it is deactivated automatically. (Service Accounts [non-human] will have a 365-day inactive period.)

Note: If a team member leaves the CMIPS Operations team, all machine passwords must be reset within 30 days, using policy requirements included in the System Administration Plan.

DSD 6/Architecture – System Security/Business Processes /Business Rules/Cúram Tables with Audit Turned On

CI	Document Name
CI-117877 - DSD BR Cram Tables with Audit Turned On IMPLEMENTED	DSD_BR_Cúram_Tables_with_Audit_Turned_On.doc

Cúram tables within the CMIPS may have the "Audit" feature turned on as a configuration setting and will track changes in the Audit XML. Specific tables will be determined based upon the need for history and security tracking. This capability may change through development, testing, and performance tuning. If the capability changes, then CGI requests approval from the CMIPS Project Director to modify the auditing configuration.

DSD 6/Architecture – System Security/Business Processes /Business Rules/Effective Dating

CI	Document Name
CI-118126 - DSD BR Effective Dating IMPLEMENTED	DSD_BR_Effective_Dating.doc

The Web Portal has several start and end date pairs for access to the Web Portal, Web Portal Roles, Case Management, and Reporting. In all cases, the default values of the start and end date fields are blank and are not required if both fields are left blank. If one of the date fields has a date value entered, both start and end dates are required and the end date cannot be prior to the start date.

DSD 6/Architecture – System Security/Business Processes /Business Rules/Business Rules

- DSD 6/Architecture – System Security/Business Processes/Business Rules/Business Rules (1-10)
- DSD 6/Architecture – System Security/Business Processes/Business Rules/Business Rules (11-20)
- DSD 6/Architecture – System Security/Business Processes/Business Rules/Business Rules (21-30)

The following Business Rules applies to Web Portal Security Administration processes:

ID	Requirement ID	CI	Description	When	Action
1	12745	CI-111555 - DSD BR SS 01 IMPLEMENTED	Upon a third failed log in attempt, lock the user's account	On the CMIPS Dynamic Web Portal Home (Unsecure) Screen, when a User fails to enter a correct User ID and Password on the third attempt.	Lock the User's account. See error message #3.
2	12726	CI-111556 - DSD BR SS 02 IMPLEMENTED	Upon failure to correctly answer challenge questions for password reset, lock the CMIPS user's account	On the Challenge Question screen, when a user fails to correctly answer the final two challenge questions.	Lock the User's account. See error message #3.
3	12742	CI-111557 - DSD BR SS 03 IMPLEMENTED	CMIPS user accounts that are inactive for 90 days are automatically deactivated	A user has not accessed the system for 90 days	Deactivate the User's account.
4	12742	CI-111558 - DSD BR SS 04 IMPLEMENTED	Deactivate a new CMIPS account after 30 days if user does not log in	A new user has not accessed the system for 30 days	Deactivate the User's account.
5	12756	CI-111559 - DSD BR SS 05 IMPLEMENTED	Add Cúram user based upon a new user added in the CMIPS II Dynamic Web Portal with Case Management access	Create User	Add user in Cúram to the correct County as a default user.
6	12756	CI-111560 - DSD BR SS 06 IMPLEMENTED	Add BusinessObjects user based upon a new user added in the CMIPS II Dynamic Web Portal with Reports access	Create User	Add user to Business Objects.
7	12756	CI-111561 - DSD BR SS 07 IMPLEMENTED	Add Advantage HRM (payroll) user based upon a new User added in the CMIPS II Dynamic Web Portal with Advantage HRM access	Create User	Add user to Advantage HRM.
8	12756	CI-111562 - DSD BR SS 08 IMPLEMENTED	Add Advantage Financial user based upon a new user added in the CMIPS II Dynamic Web Portal with Advantage Financial access	Create User	Add user to Advantage Financial.
9	12756	CI-111563 - DSD BR SS 09 IMPLEMENTED	Delete TPF Timesheet Reporting Facility Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to TPF is removed from CMIPS Web Portal.
10	12756	CI-111564 - DSD BR SS 10 IMPLEMENTED	Delete Case Management Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to Case Management is removed from CMIPS II Web Portal.

ID	Requirement ID	CI	Description	When	Action
11	12756	CI-111565 - DSD BR SS 11 IMPLEMENTED	Delete Reporting Business Objects Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to Business Objects is removed from CMIPS II Web Portal.
12	12756	CI-111566 - DSD BR SS 12 IMPLEMENTED	Delete Advantage HRM (payroll) Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to Advantage HRM (payroll) is removed from CMIPS II Web Portal.

13	12756	CI-111567 - DSD BR SS 13 IMPLEMENTED	Delete Advantage Financial Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to Advantage Financial is removed from CMIPS II Web Portal.
14	12756	CI-111568 - DSD BR SS 14 IMPLEMENTED	Update the RD_User table for any user whose Reports access is added or removed from the CMIPS II Web Portal	Update User Profile	Update the RD_User table.
15	12756	CI-111569 - DSD BR SS 15 IMPLEMENTED	If a user is not created successfully in Cúram or BusinessObjects, remove the indicated access dates for the associated application	When a failed attempt is made to add a user in Cúram or Business Objects	Remove the Start and End Date for Cúram or Business Objects from the user's security profile.
16	16878 12741	CI-111570 - DSD BR SS 16 IMPLEMENTED	Display Reset Password if password is expired or due to expire within five days	Upon successful logon and password is expired or due to expire within five days	Display the Reset Password screen. If the pre-expire flag is indicated, reset the pre-expire flag upon successful password update.
17	12756 16878 12748	CI-111571 - DSD BR SS 17 IMPLEMENTED	First time a user logs into the CMIPS II Web Portal, display the Maintain Account screen after successful login	When a user logs into the CMIPS II Dynamic Web Portal for the first time	Display the Maintain Account screen, then flow to the Home page (secure).
18	16878 12735	CI-111572 - DSD BR SS 18 IMPLEMENTED	Generate system assigned password for CMIPS II Web Portal	Upon the following conditions: Adding a new user to the CMIPS II Web Portal Reactivating a user on the CMIPS II Web Portal	Generate and display a new system assigned password.
19	12756	CI-111573 - DSD BR SS 19 IMPLEMENTED	Filter for CMIPS II Dynamic Web Portal Roles drop-down list	Upon display of Create User and Update User Profile screens	If User is County Security Officer or County Security Administrator, do not display the following CMIPS II Dynamic Web Portal Roles: Security Officer Advantage HRM (payroll) Advantage Financial Web Portal Master TPF Manager
20	12741	CI-111574 - DSD BR SS 20 IMPLEMENTED	Display Reset Password upon first time a user logs into CMIPS II Web Portal.	Upon 1st log in to the CMIPS II Web Portal, new user must reset their password.	Upon 1st log in, new user must reset their password.

ID	Requirement ID	CI	Description	When	Action
21	12726 12756	CI-111575 - DSD BR SS 21 IMPLEMENTED	Reset the user account for CMIPS II Dynamic Web Portal Locked indicator	When the password for the CMIPS II Dynamic Web Portal is being reset by the Security Administrator /Officer	Reset the account Lock indicator.
22	12756 16829	CI-116766 - DSD BR SS 22 IMPLEMENTED	Create User – CMIPS II Web Portal Display User Name in All Uppercase Letters	When the Create link is selected on the Create User screen and lowercase letters were used when entering the following fields: • Last Name • First Name • Middle Name	Display the First Name, Last Name and Middle Name entries in all uppercase letters on the Maintain Account Information screen.
23	16829 12756	CI-116767 - DSD BR SS 23 IMPLEMENTED	Update User Profile – CMIPS II Web Portal Display User Name in All Uppercase Letters	When the Update link is selected on the Update User Profile screen and lowercase letters were used when entering the following fields: • Last Name • First Name • Middle Name	Display the First Name, Last Name and Middle Name entries in all uppercase letters on the Maintain Account Information screen.
24	12724 12747	CI-215794 - DSD BR SS 24 IMPLEMENTED	Upon Timeout of CMIPS II Dynamic Web Portal session	When the user has not taken any action in the CMIPS II Dynamic Web Portal for 20 minutes	Display the following message: "CMIPS II Session Timed out. You are successfully logged out of CMIPS II." User must then select Close Browser, and the browser session is closed.

DSD 6/Architecture – System Security/Business Processes /Business Rules/Business Rules (1-10)

The following Business Rules applies to Web Portal Security Administration processes:

ID	Requirement ID	CI	Description	When	Action
1	12745	CI-111555 - DSD BR SS 01 IMPLEMENTED	Upon a third failed log in attempt, lock the user's account	On the CMIPS Dynamic Web Portal Home (Unsecure) Screen, when a User fails to enter a correct User ID and Password on the third attempt.	Lock the User's account. See error message #3.
2	12726	CI-111556 - DSD BR SS 02 IMPLEMENTED	Upon failure to correctly answer challenge questions for password reset, lock the CMIPS user's account	On the Challenge Question screen, when a user fails to correctly answer the final two challenge questions.	Lock the User's account. See error message #3.
3	12742	CI-111557 - DSD BR SS 03 IMPLEMENTED	CMIPS user accounts that are inactive for 90 days are automatically deactivated	A user has not accessed the system for 90 days	Deactivate the User's account.
4	12742	CI-111558 - DSD BR SS 04 IMPLEMENTED	Deactivate a new CMIPS account after 30 days if user does not log in	A new user has not accessed the system for 30 days	Deactivate the User's account.
5	12756	CI-111559 - DSD BR SS 05 IMPLEMENTED	Add Cúram user based upon a new user added in the CMIPS II Dynamic Web Portal with Case Management access	Create User	Add user in Cúram to the correct County as a default user.
6	12756	CI-111560 - DSD BR SS 06 IMPLEMENTED	Add BusinessObjects user based upon a new user added in the CMIPS II Dynamic Web Portal with Reports access	Create User	Add user to Business Objects.
7	12756	CI-111561 - DSD BR SS 07 IMPLEMENTED	Add Advantage HRM (payroll) user based upon a new User added in the CMIPS II Dynamic Web Portal with Advantage HRM access	Create User	Add user to Advantage HRM.
8	12756	CI-111562 - DSD BR SS 08 IMPLEMENTED	Add Advantage Financial user based upon a new user added in the CMIPS II Dynamic Web Portal with Advantage Financial access	Create User	Add user to Advantage Financial.
9	12756	CI-111563 - DSD BR SS 09 IMPLEMENTED	Delete TPF Timesheet Reporting Facility Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to TPF is removed from CMIPS Web Portal.
10	12756	CI-111564 - DSD BR SS 10 IMPLEMENTED	Delete Case Management Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to Case Management is removed from CMIPS II Web Portal.

DSD 6/Architecture – System Security/Business Processes /Business Rules/Business Rules (11-20)

ID	Requirement ID	CI	Description	When	Action
11	12756	CI-111565 - DSD BR SS 11 IMPLEMENTED	Delete Reporting Business Objects Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to Business Objects is removed from CMIPS II Web Portal.
12	12756	CI-111566 - DSD BR SS 12 IMPLEMENTED	Delete Advantage HRM (payroll) Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to Advantage HRM (payroll) is removed from CMIPS II Web Portal.
13	12756	CI-111567 - DSD BR SS 13 IMPLEMENTED	Delete Advantage Financial Role from CMIPS II Dynamic Web Portal	Update User Profile	User access to Advantage Financial is removed from CMIPS II Web Portal.
14	12756	CI-111568 - DSD BR SS 14 IMPLEMENTED	Update the RD_User table for any user whose Reports access is added or removed from the CMIPS II Web Portal	Update User Profile	Update the RD_User table.
15	12756	CI-111569 - DSD BR SS 15 IMPLEMENTED	If a user is not created successfully in Cúram or BusinessObjects, remove the indicated access dates for the associated application	When a failed attempt is made to add a user in Cúram or Business Objects	Remove the Start and End Date for Cúram or Business Objects from the user's security profile.
16	16878 12741	CI-111570 - DSD BR SS 16 IMPLEMENTED	Display Reset Password if password is expired or due to expire within five days	Upon successful logon and password is expired or due to expire within five days	Display the Reset Password screen. If the pre-expire flag is indicated, reset the pre-expire flag upon successful password update.
17	12756 16878 12748	CI-111571 - DSD BR SS 17 IMPLEMENTED	First time a user logs into the CMIPS II Web Portal, display the Maintain Account screen after successful login	When a user logs into the CMIPS II Dynamic Web Portal for the first time	Display the Maintain Account screen, then flow to the Home page (secure).
18	16878 12735	CI-111572 - DSD BR SS 18 IMPLEMENTED	Generate system assigned password for CMIPS II Web Portal	Upon the following conditions: Adding a new user to the CMIPS II Web Portal Reactivating a user on the CMIPS II Web Portal	Generate and display a new system assigned password.
19	12756	CI-111573 - DSD BR SS 19 IMPLEMENTED	Filter for CMIPS II Dynamic Web Portal Roles drop-down list	Upon display of Create User and Update User Profile screens	If User is County Security Officer or County Security Administrator, do not display the following CMIPS II Dynamic Web Portal Roles: Security Officer Advantage HRM (payroll) Advantage Financial Web Portal Master TPF Manager
20	12741	CI-111574 - DSD BR SS 20 IMPLEMENTED	Display Reset Password upon first time a user logs into CMIPS II Web Portal.	Upon 1st log in to the CMIPS II Web Portal, new user must reset their password.	Upon 1st log in, new user must reset their password.

DSD 6/Architecture – System Security/Business Processes /Business Rules/Business Rules (21-30)

ID	Requirement ID	CI	Description	When	Action
21	12726 12756	CI-111575 - DSD BR SS 21 IMPLEMENTED	Reset the user account for CMIPS II Dynamic Web Portal Locked indicator	When the password for the CMIPS II Dynamic Web Portal is being reset by the Security Administrator /Officer	Reset the account Lock indicator.
22	12756 16829	CI-116766 - DSD BR SS 22 IMPLEMENTED	Create User – CMIPS II Web Portal Display User Name in All Uppercase Letters	When the Create link is selected on the Create User screen and lowercase letters were used when entering the following fields: • Last Name • First Name • Middle Name	Display the First Name, Last Name and Middle Name entries in all uppercase letters on the Maintain Account Information screen.
23	16829 12756	CI-116767 - DSD BR SS 23 IMPLEMENTED	Update User Profile – CMIPS II Web Portal Display User Name in All Uppercase Letters	When the Update link is selected on the Update User Profile screen and lowercase letters were used when entering the following fields: • Last Name • First Name • Middle Name	Display the First Name, Last Name and Middle Name entries in all uppercase letters on the Maintain Account Information screen.
24	12724 12747	CI-215794 - DSD BR SS 24 IMPLEMENTED	Upon Timeout of CMIPS II Dynamic Web Portal session	When the user has not taken any action in the CMIPS II Dynamic Web Portal for 20 minutes	Display the following message: "CMIPS II Session Timed out. You are successfully logged out of CMIPS II." User must then select Close Browser, and the browser session is closed.

DSD 6/Architecture – System Security/Business Processes /Tasks/Notifications

There are no tasks or notifications currently defined.

DSD 6/Architecture – System Security/Business Processes /Internal Interfaces

The following interfaces are developed to support the previously defined processes.

1. Operational data transfer to the Reporting Database
2. ETL scheduling and description is defined in the Operations Plan (CMIPShare > Document Center > Deliverables > 6.1-01 Operations Plan).
3. Custom Security API to and from CMIPS II Dynamic Web Portal to Cúram

The figure below shows the flow of data from the operational databases to the Reporting Database (Online Archive). The ETL scripts are run and scheduled by the IBM InfoSphere for Cúram and AutoSys for CGI Advantage.

CI	Document Name
CI-117893 - DSD INTF Operational data transfer to the Reporting Database IMPLEMENTED	DSD_INTF_Operational_data_transfer_to_the_Reporting_Database.doc

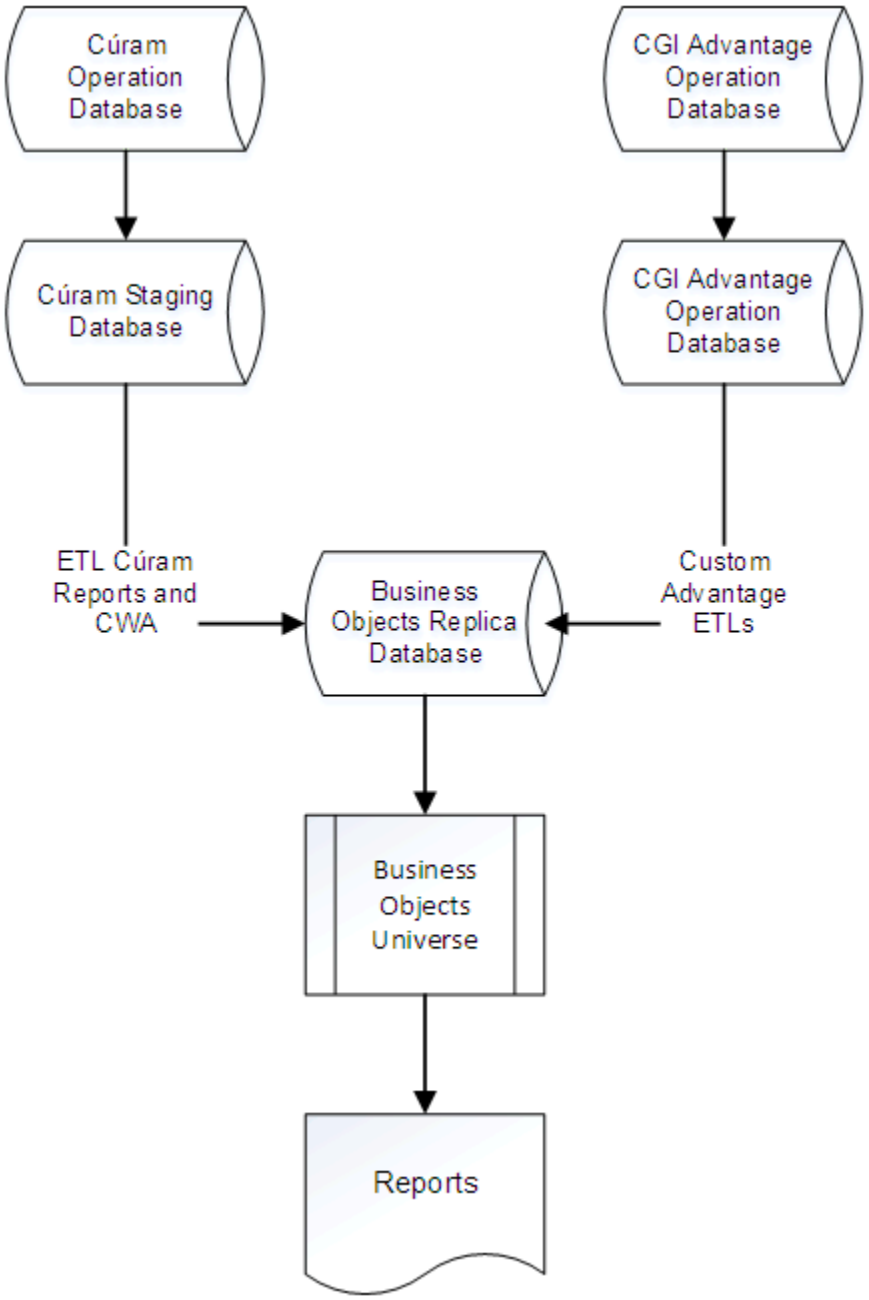


Figure – ETL Data Flow

DSD 6/Architecture – System Security/Business Processes /Internal Interfaces/API Structure from CMIPS II Dynamic Web Portal to Cúram

CI	Document Name
CI-106273 - DSD INTF API Structure from CMIPS II Web Portal to Curam IMPLEMENTED	DSD_INTF_API_Structure_from_CMIPS_II_Web_Portal_to_Curam.doc

The Cúram API is invoked as part of a creating a new user, reactivating a user or a change in security profile to ensure that the Web Portal and Cúram are in sync with the user ID. The portal performs the authentication and authorization, and transfers the authentication to Cúram and BusinessObjects via secure machine-to-machine authentication. The URI of the transfer includes the user ID, but not the password. Passwords are housed as part of the Web Portal LDAP security schema.

The communication for this API is a synchronous transaction where the send XML is provided, updated by Cúram then return the same XML with updated status code.

Send XML

Name	Acceptable Values	Value Type	Format (as required)
TransactionID	CúramNewUser	Text	NA
userName	Alphanumeric of 30 characters in length	Text	First letter of first name Up to seven characters of last name Two digits for uniqueness
countyCode	Numeric [0-99]	Integer	Cúram table of counties
status	Number [0-9]	Integer	1=initiated
firstName	Alphanumeric of 25 characters in length	Text	
lastName	Alphanumeric of 30 characters in length	Text	

Return XML

Name	Acceptable Values	Value Type	Format (as required)
TransactionID	CúramNewUser	Text	Same as send
userName	Alphanumeric of 30 characters in length	Text	Same as send
countyCode	Numeric [0-99]	Integer	Same as send
status	Number [0-9]	Integer	2=Success 3=Already exists 4=Failed due to invalid user role 5=failed due to invalid county 6=Failed undefined reason 7 = Invalid position 8 = Concernrole failed 9 = Encryption failed 10 = County-level organization unit location missing
firstName	Alphanumeric of 25 characters in length	Text	
lastName	Alphanumeric of 30 characters in length	Text	

DSD 6/Architecture – System Security/Business Processes /External Interfaces

The standard for security communications for the CMIPS interfaces is:

- Internal to California Department of Technology (CDT) Data Center Firewalls:
- BAW HTTP: Business Automation Workflow (BAW) connects to the CGI-hosted application and puts/pulls files using HTTP/HTTPS/SOAP protocol
    - BAW SFTP: BAW connects to the CDT-hosted application and puts/pulls files using secure FTP protocol
    - BAW SFTP: BAW connects to an external partners CDT-hosted application and puts/pulls files using secure FTP protocol
    - BAW File: BAW executes a read or write to files from a CGI-hosted server files share

Note: 256 bit encryption is the preferred configuration.

DSD 6/Architecture – System Security/Business Processes /External Interfaces/External to CGI Data Center Firewalls

- BAW HTTPS: BAW connects to the External Hosted application and puts/pulls files using HTTPS/SOAP protocol
- BAW SFTP: BAW connects to CDT Hosted Application and puts/pulls files using secure FTP protocol

Note: A matrix of each interface indicating the availability of the connection security protocol in the order of preference, and selected security protocol is located in the Interface Detail Design in the section labeled "Characteristics of the Interface" for each interface (see interfaces documented in IDD Part 2 and IDD Part 3).

DSD 6/Architecture – System Security/Business Processes /Batch Processing

The following batch jobs are used to transfer security-related data to for the reports required by SOW and SyRS.

Batch Process Name	CI	Description	Estimated Size (Records)	Frequency	Send Receive Maintenance
Cúram Security Audit XML	CI-116251 - DSD BTCH Curam Security Audit XML IMPLEMENTED	Transfer data from the Operational Cúram Database on all tables with security audit to the Reporting DB	Change Records per day	Daily	Maintenance

DSD 6/Architecture – System Security/Business Processes /Application Security Roles

DSD 6/Architecture – System Security/Business Processes /Application Security Roles/Cúram Security Roles

Refer to Appendix A of this document for the Cúram Security Roles.

DSD 6/Architecture – System Security/Business Processes /Application Security Roles/Cúram Security Groups

Refer to Appendix A of this document for Cúram Security Groups.

DSD 6/Architecture – System Security/Business Processes /Application Security Roles/Location Based Security – Cúram

CI	Document Name
CI-106699 - DSD SecRoles Location Based Security Curam IMPLEMENTED	DSD_SecRoles_Location_Based_Security_Curam.doc

Location Based Security augments the Role Based Security by creating further security granularity based on locations. Example: A social worker can see a case in another district office, but cannot update the case.

Location Based Security within Cúram is defined at the State, County and District Office levels. Location Based Security is utilized in addition to Cúram Role Based security. CMIPS controls user access to view specific case information based upon the following:

- Verify the user has access to the screen based upon his/her security role.
- Verify the user has access to view the case based upon the location of the case (county and district office) and the defined location for the user (state, county or district office).

Based upon the CMIPS Location Based Security option of 'Read Only', each user is only able to update case information for cases assigned within their county or district office. Users are able to view case information Statewide based upon the screens available to them through their security roles.

Provider information is an exception to this, in that Providers may work for multiple cases across multiple counties and are not assigned to a single county or district office. If a user is assigned the security role to update Provider information, they are able to update any Provider's demographic information. Information relating to a Provider that is case specific, such as assigned hours, is limited to those users within the county or district office associated with the case.

Note: Each person can only have one role assigned in Cúram.

DSD 6/Architecture – System Security/Business Processes /Application Security Roles/Web Portal Security Roles

CI	Document Name
CI-106703 - DSD SecRoles Web Portal Security Roles IMPLEMENTED	DSD_SecRoles_Web_Portal_Security_Roles.doc

The following matrix represents the unique security roles defined within the Web Portal. Each user may be assigned more than one of these roles.

Role	Description
Case Management	User has access to CMIPS Case Management application.
Reporting	User has access to CMIPS Reporting through BusinessObjects.
Web Portal	User has access to base Web Portal screens (Reset Password, Help, Notifications, contacts, Maintain Account Information).
Advantage HRM	User has access to Advantage HRM application.
Advantage Financial	User has access to Advantage Financial application.
Query and Sampling	User has access to the Query and Sampling screens (Reports, Criteria, Form SOC 293, Form SOC 426, Sampling and Tasks screens).
Security Officer	User has access to Security Administration screens (Add New User, Security Profile, Reset User Password and Report Security).
Security Administrator	User has access to Security Administration screens (Security Profile and Reset User Password, Report Security).
Web Master	User has access to maintain Web Portal Content.
TPF Manager	User has access to TPF Metrics add and modify screens.

DSD 6/Architecture – System Security/Business Processes /Application Security Roles/Business Objects Security Roles

CI	Document Name
CI-106700 - DSD SecRoles Business Objects Security Roles IMPLEMENTED	DSD_SecRoles_Business_Objects_Security_Roles.doc

The following matrix represents the unique security groups and associated folders defined within Business Objects. Each user may be assigned one or more of these groups.

Group	Folders (Reports)
State	State Only
	Case Maintenance
	Homemaker Reports
	Payroll
	Provider Management
	QA/Fraud
	Time and Attendance
	Health Benefit Managers
	Labor Organizations
Core	Case Maintenance
	Homemaker Reports
	Payroll
	Provider Management
	QA/Fraud
	Time and Attendance
Health Benefit Manager	Health Benefit Managers
Labor Organization	Labor Organizations
County Administrator	System Performance
	System Security
	Data Download
	Data Retention
Internal CGI	System Performance
	System Security
	Data Download
	Data Retention
	State Only
	Case Maintenance
	Homemaker Reports
	Payroll
	Provider Management

	QA/Fraud
	Time and Attendance
	Health Benefit Managers
	Labor Organizations
WPCS	WPCS

DSD 6/Architecture – System Security/Business Processes /Reporting

All CMIPS reports that support System Security are located in the current approved version of the System Security Plan (CMIPShare > Document Center > Deliverables > 6.7-01 System Security Plan).

DSD 6/Architecture – System Security/Business Processes /Forms

Security DSD does not use forms in its solution.

DSD 6/Architecture – System Security/Code Table Definitions

This section documents each of the code tables and their values and descriptions that are utilized by the CMIPS solution.

The following Code Tables are utilized by the System Administration – Security.

Table – Code Table: County

CI	Document Name
CI-121491 - DSD CT County Portal IMPLEMENTED	DSD_CT_County_Portal.doc

Code Value	Code Description	Default Value	Sort Order	Parent Code	Enabled	Notes
01	Alameda	No	1	No	Yes	
02	Alpine	No	2	No	Yes	
03	Amador	No	3	No	Yes	
04	Butte	No	4	No	Yes	
05	Calaveras	No	5	No	Yes	
06	Colusa	No	6	No	Yes	
07	Contra Costa	No	7	No	Yes	
08	Del Norte	No	8	No	Yes	
09	El Dorado	No	9	No	Yes	
10	Fresno	No	10	No	Yes	
11	Glenn	No	11	No	Yes	
12	Humboldt	No	12	No	Yes	
13	Imperial	No	13	No	Yes	
14	Inyo	No	14	No	Yes	
15	Kern	No	15	No	Yes	
16	Kings	No	16	No	Yes	
17	Lake	No	17	No	Yes	
18	Lassen	No	18	No	Yes	
19	Los Angeles	No	19	No	Yes	
20	Madera	No	20	No	Yes	
21	Marin	No	21	No	Yes	
22	Mariposa	No	22	No	Yes	
23	Mendocino	No	23	No	Yes	
24	Merced	No	24	No	Yes	
25	Modoc	No	25	No	Yes	
26	Mono	No	26	No	Yes	
27	Monterey	No	27	No	Yes	
28	Napa	No	28	No	Yes	
29	Nevada	No	29	No	Yes	
30	Orange	No	30	No	Yes	
31	Placer	No	31	No	Yes	
32	Plumas	No	32	No	Yes	
33	Riverside	No	33	No	Yes	
34	Sacramento	No	34	No	Yes	

35	San Benito	No	35	No	Yes	
36	San Bernardino	No	36	No	Yes	
37	San Diego	No	37	No	Yes	
38	San Francisco	No	38	No	Yes	
39	San Joaquin	No	39	No	Yes	
40	San Luis Obispo	No	40	No	Yes	
41	San Mateo	No	41	No	Yes	
42	Santa Barbara	No	42	No	Yes	
43	Santa Clara	No	43	No	Yes	
44	Santa Cruz	No	44	No	Yes	
45	Shasta	No	45	No	Yes	
46	Sierra	No	46	No	Yes	
47	Siskiyou	No	47	No	Yes	
48	Solano	No	48	No	Yes	
49	Sonoma	No	49	No	Yes	
50	Stanislaus	No	50	No	Yes	
51	Sutter	No	51	No	Yes	
52	Tehama	No	52	No	Yes	
53	Trinity	No	53	No	Yes	
54	Tulare	No	54	No	Yes	
55	Tuolumne	No	55	No	Yes	
56	Ventura	No	56	No	Yes	
57	Yolo	No	57	No	Yes	
58	Yuba	No	58	No	Yes	
99	All Counties	No	59	No	Yes	

Table – Java Code Table: CMIPS II Portal Roles

CI	Document Name
CI-116338 - DSD CT CMIPS II Portal Roles IMPLEMENTED	DSD_CT_CMIPS_II_Portal_Roles.doc

Code Value	Code Description	Default Value	Sort Order	Parent Code	Enabled	Notes
QuerySamplingTool	QuerySamplingTool	No	1	No	Yes	
DataRetention	DataRetention	No	2	No	Yes	
SecurityAdministrator	SecurityAdministrator	No	3	No	Yes	Can reset password and update access.
SecurityOfficer	SecurityOfficer	No	4	No	Yes	Can create new users and reactivate users.
WebMasterUsers	WebMasterUsers	No	5	No	Yes	
TPFManager	TPFManager	No	6	No	Yes	
AdvantageFinancial	AdvantageFinancial	No	7	No	Yes	
AdvantageHRM	AdvantageHRM	No	8	No	Yes	Payroll

Table – Java Code Table: Report Access Level

CI	Document Name
CI-116339 - DSD CT Report Access Level IMPLEMENTED	DSD_CT_Report_Access_Level.doc

Code Value	Code Description	Default Value	Sort Order	Parent Code	Enabled	Notes
0 – State	0 – State	No	1	No	Yes	User may view report data statewide.
1 - County	1 – County	No	2	No	Yes	User may view report data within their county only.
2 - Worker	2 – Worker	No	3	No	Yes	User may view only their own worker-level report data.

DSD 6/Architecture – System Security/Database Entities

Table – LDAP Database design

Screen Name	Screen Element	Data Field - Source of Data	Server/Table	Attribute /Column Name
Log On Screen	User ID	User ID	LDAP Server	Attribute: uid
	Encrypted Password	Character	LDAP Server	Attribute: userpassword
Get Challenge Question Screen	User ID	User ID	LDAP Server	Attribute: uid
	Challenge Question 1	Lookup	SM_WAN_User	SM_WAN_UserChQues1
	Challenge Answer 1	Short Text	SM_WAN_User	SM_WAN_UserChAns1
	Challenge Question 2	Lookup	SM_WAN_User	SM_WAN_UserChQues2
	Challenge Answer 2	Short Text	SM_WAN_User	SM_WAN_UserChAns2
	Challenge Question 3	Lookup	SM_WAN_User	SM_WAN_UserChQues3
	Challenge Answer 3	Short Text	SM_WAN_User	SM_WAN_UserChAns3
User Profile Screen	User ID	User ID	LDAP server	Attribute: uid
	Date Account effective	Date	SM_WAN_User	SM_WAN_DateEff
	Date Account Disable	Date	SM_WAN_User	SM_WAN_DateDis
	Pre-expired Logon Flag	Flag	SM_WAN_User	SM_WAN_PreExpFlag
	Date Pre-Expire Activated	Date	SM_WAN_User	SM_WAN_PreExpDate
	Date Last Log on Success	Date	SM_WAN_User	SM_WAN_LastLogOn
	Lock-out Flag	Flag	SM_WAN_User	SM_WAN_LockOutFlag
	Failed attempt count	Counter	SM_WAN_User	SM_WAN_PWFACounter
	Worker Number	Integer	LDAP Server	Attribute: workerNumber
	County	Integer	LDAP Server	All groups under Organization: Counties
	Location	Lookup	SM_WAN_User	SM_WAN_Location
	Authorizing Supervisor ID	Lookup	SM_WAN_User	SM_AUTHORIZING_MGR
	First Name	Short Character	LDAP server	Attribute: givenName
	Last Name	Short Character	LDAP Server	Attribute: sn
	Middle Name	Short Character	LDAP Server	Attribute: middlename
	Day of Birth	Integer	LDAP Server	Attribute: dayOfBirth
	Month of Birth	Integer	LDAP Server	Attribute: monthOfBirth
	Date Case Management Access Start	Date	LDAP Server	Attribute: datestartcm
	Date Case Management Access End	Date	LDAP Server	Attribute: dateendcm
	Date BusinessObjects Access Start	Date	LDAP Server	Attribute: datestartbo
	Date BusinessObjects Access End	Date	LDAP Server	Attribute: dateendbo
	Date Web Portal Access Start	Date	LDAP Server	Attribute: datestartwp
	Date Web Portal Access End	Date	LDAP Server	Attribute: dateendwp
	Inactive Flag Set	Flag	SM_WAN_User	SM_WAN_Inactive_Flag
	Portal Role 1	Pull Down	Web Portal	Hardcoded
	Portal Role 1 start date	Date	LDAP Server	Attribute: datestartpr1
	Portal Role 1 end Date	Date	LDAP Server	Attribute: dateendpr1
	Portal Role 2	Pull Down	Web Portal	Hardcoded
	Portal Role 2 start date	Date	LDAP Server	Attribute: datestartpr2
	Portal Role 2 end Date	Date	LDAP Server	Attribute: dateendpr2

	Portal Role 3	Pull Down	Web Portal	Hardcoded
	Portal Role 3 start date	Date	LDAP Server	Attribute: datestartpr3
	Portal Role 3 end Date	Date	LDAP Server	Attribute: dateendpr3
	Portal Role 4	Pull Down	Web Portal	Hardcoded
	Portal Role 4 start date	Date	LDAP Server	Attribute: datestartpr4
	Portal Role 4 end Date	Date	LDAP Server	Attribute: dateendpr4
	Portal Role 5	Pull Down	Web Portal	Hardcoded
	Portal Role 5 start date	Date	LDAP Server	Attribute: datestartpr5
	Portal Role 5 end Date	Date	LDAP Server	Attribute: dateendpr5
	Portal Role 6	Pull Down	Web Portal	Hardcoded
	Portal Role 6 start date	Date	LDAP Server	Attribute: datestartpr6
	Portal Role 6 end Date	Date	LDAP Server	Attribute: dateendpr6
	Portal Role 7	Pull Down	Web Portal	Hardcoded
	Portal Role 7 start date	Date	LDAP Server	Attribute: datestartpr7
	Portal Role 7 end Date	Date	LDAP Server	Attribute: dateendpr7
	Portal Role 8	Pull Down	Web Portal	Hardcoded
	Portal Role 8 start date	Date	LDAP Server	Attribute: datestartpr8
	Portal Role 8 end Date	Date	LDAP Server	Attribute: dateendpr8
	Your Password	Short Character	LDAP Server	Attribute: userpassword
	Report Access Level	Drop-down	RD_USERSECURITY	Data_Viewability
Enter New Password	New Password	Encrypted	LDAP Server	Attribute: userpassword
	Verify Password	Encrypted	-	-
	Date Last Used Old Password 0	Date	LDAP Server Password Policy	Operational attribute: pwdHistory
	Old password 1	Encrypted	LDAP Server Password Policy	Operational attribute: pwdHistory
	Date Last Used Old Password 1	Date	LDAP Server Password Policy	Operational attribute: pwdHistory
	Old password 2	Encrypted	LDAP Server Password Policy	Operational attribute: pwdHistory
	Date Last Used Old Password 2	Date	LDAP Server Password Policy	Operational attribute: pwdHistory
	Old password 3	Encrypted	LDAP Server Password Policy	Operational attribute: pwdHistory
	Date Last Used Old Password 3	Date	LDAP Server Password Policy	Operational attribute: pwdHistory
	Old password 4	Encrypted	LDAP Server Password Policy	Operational attribute: pwdHistory
	Date Last Used Old Password 4	Date	LDAP Server Password Policy	Operational attribute: pwdHistory
	Old password 5	Encrypted	LDAP Server Password Policy	Operational attribute: pwdHistory
	Date Last Used Old Password 5	Date	LDAP Server Password Policy	Operational attribute: pwdHistory
	Old password 6	Encrypted	LDAP Server Password Policy	Operational attribute: pwdHistory
	Date Last Used Old Password 6	Date	LDAP Server Password Policy	Operational attribute: pwdHistory
	Old password 7	Encrypted	LDAP Server Password Policy	Operational attribute: pwdHistory
	Date Last Used Old Password 7	Date	LDAP Server Password Policy	Operational attribute: pwdHistory

	Old password 8	Encrypted	LDAP Server Password Policy	Operational attribute: pwdHistory
	Date Last Used Old Password 8	Date	LDAP Server Password Policy	Operational attribute: pwdHistory
	Old password 9	Encrypted	LDAP Server Password Policy	Operational attribute: pwdHistory
	Date Last Used Old Password 9	Date	LDAP Server Password Policy	Operational attribute: pwdHistory
Maintain Account Information	User ID	User ID	LDAP Server	Attribute: uid
	Worker Number	Integer	LDAP Server	Attribute: workerNumber
	First Name	Short Character	LDAP Server	Attribute: givenName
	Last Name	Short Character	LDAP Server	Attribute: sn
	Middle Name	Short Character	LDAP Server	Attribute: middleName
	Authorizing Supervisor ID	Lookup	SM_WAN_User	SM_AUTHORIZING_MGR
	County	Lookup	LDAP Server	All groups under Organization: Counties
	Location	Lookup	SM_WAN_User	SM_WAN_Location
	Office Mail Address	Address	SM_WAN_User	SM_WAN_Address
	Office Phone(s)	Integer	SM_WAN_User	SM_WAN_AddNum
	Office Email	Short Character	SM_WAN_User	SM_WAN_Email
	City	Short Character	SM_WAN_User	SM_WAN_City
	State	Short Character	SM_WAN_User	SM_WAN_State
	ZIP	Integer	SM_WAN_User	SM_WAN_Zip
	ZIP plus four	Integer	SM_WAN_User	SM_WAN_Zip_Plus_Four
	Challenge Question 1	Lookup	SM_WAN_User	SM_WAN_UserChQues1
	Challenge Answer 1	Short Text	SM_WAN_User	SM_WAN_UserChAns1
	Challenge Question 2	Lookup	SM_WAN_User	SM_WAN_UserChQues2
	Challenge Answer 2	Short Text	SM_WAN_User	SM_WAN_UserChAns2
	Challenge Question 3	Lookup	SM_WAN_User	SM_WAN_UserChQues3
	Challenge Answer 3	Short Text	SM_WAN_User	SM_WAN_UserChAns3
	Password	Short Character	LDAP Server	Attribute: userpassword
Search End User screen	User ID	User ID	LDAP Server	Attribute: uid
	Worker Number	Integer	LDAP Server	Attribute: workerNumber
	First Name	Short Character	LDAP Server	Attribute: givenName
	Last Name	Short Character	LDAP Server	Attribute: sn
	Middle Name	Short Character	LDAP Server	Attribute: middleName
	County	Integer	LDAP Server	All groups under Organization: Counties
Verify User Screen	User ID	User ID	LDAP Server	Attribute: uid
	Worker Number	Integer	LDAP Server	Attribute: workerNumber
	First Name	Short Character	LDAP Server	Attribute: givenName
	Last Name	Short Character	LDAP Server	Attribute: sn
	Middle Name	Short Character	LDAP Server	Attribute: middleName
	County	Lookup	LDAP Server	All groups under Organization: Counties
	Location	Lookup	SM_WAN_User	SM_WAN_Location
	Office Mail Address	Address	SM_WAN_User	SM_WAN_Address

	Office Phone(s)	Integer	SM_WAN_User	SM_WAN_AddNum
	Office Email	Short Character	SM_WAN_User	SM_WAN_Email
	City	Short Character	SM_WAN_User	SM_WAN_City
	State	Short Character	SM_WAN_User	SM_WAN_State
	ZIP	Integer	SM_WAN_User	SM_WAN_Zip
	ZIP plus four	Integer	SM_WAN_User	SM_WAN_Zip_Plus_Four
	Date Password Last Changed	Date	SM_WAN_User	SM_WAN_Date_PW_Changed
System Assigned Password Screen	User ID	User ID	LDAP server	Attribute: uid
	System Assigned Password	Short Character	LDAP Server	Attribute: userpassword
	System assigned password will expire on	Date	SM_WAN_User	SM_WAN_PreExpDate
	Security Officer User ID	User ID	SM_WAN_User	SM_WAN_UserID
	Your Password	Short Character	LDAP Server	Attribute: userpassword
Create User screen	User ID	User ID	LDAP Server	Attribute: uid
	System Assigned Password	Short Character	LDAP Server	Attribute: userpassword
	Date Account effective	Date	SM_WAN_User	SM_WAN_DateEff
	Date Account Disable	Date	SM_WAN_User	SM_WAN_DateDis
	Pre-expired Logon Flag	Flag	SM_WAN_User	SM_WAN_PreExpFlag
	Date Pre-Expire Activated	Date	SM_WAN_User	SM_WAN_PreExpDate
	Worker Number	Integer	LDAP Server	Attribute: workerNumber
	County	Integer	LDAP Server	All groups under Organization: Counties
	Location	Lookup	SM_WAN_User	SM_WAN_Location
	Authorizing Supervisor ID	Lookup	SM_WAN_User	SM_WAN_AUTHORIZING_MGR
	First Name	Short Character	LDAP Server	Attribute: givenName
	Last Name	Short Character	LDAP Server	Attribute: sn
	Middle Name	Short Character	LDAP Server	Attribute: middleName
	Day of Birth	Integer	LDAP Server	Attribute: dayOfBirth
	Month of Birth	Integer	LDAP Server	Attribute: monthOfBirth
	Date Case Management Access Start	Date	LDAP Server	Attribute: datestartcm
	Date Case Management Access End	Date	LDAP Server	Attribute: dateendcm
	Date BusinessObjects Access Start	Date	LDAP Server	Attribute: datestartbo
	Date BusinessObjects Access End	Date	LDAP Server	Attribute: dateendbo
	Date Web Portal Access Start	Date	LDAP Server	Attribute: datestartwp
	Date Web Portal Access End	Date	LDAP Server	Attribute: dateendwp
	Portal Role 1	Pull Down	Web Portal	Hardcoded
	Portal Role 1 start date	Date	LDAP Server	Attribute: datestartpr1
	Portal Role 1 end Date	Date	LDAP Server	Attribute: dateendpr1
	Portal Role 2	Pull Down	Web Portal	Hardcoded
	Portal Role 2 start date	Date	LDAP Server	Attribute: datestartpr2
	Portal Role 2 end Date	Date	LDAP Server	Attribute: dateendpr2
	Portal Role 3	Pull Down	Web Portal	Hardcoded
	Portal Role 3 start date	Date	LDAP Server	Attribute: datestartpr3
	Portal Role 3 end Date	Date	LDAP Server	Attribute: dateendpr3
	Portal Role 4	Pull Down	Web Portal	Hardcoded

	Portal Role 4 start date	Date	LDAP Server	Attribute: datestartpr4
	Portal Role 4 end Date	Date	LDAP Server	Attribute: dateendpr4
	Portal Role 5	Pull Down	Web Portal	Hardcoded
	Portal Role 5 start date	Date	LDAP Server	Attribute: datestartpr5
	Portal Role 5 end Date	Date	LDAP Server	Attribute: dateendpr5
	Portal Role 6	Pull Down	Web Portal	Hardcoded
	Portal Role 6 start date	Date	LDAP Server	Attribute: datestartpr6
	Portal Role 6 end Date	Date	LDAP Server	Attribute: dateendpr6
	Portal Role 7	Pull Down	Web Portal	Hardcoded
	Portal Role 7 start date	Date	LDAP Server	Attribute: datestartpr7
	Portal Role 7 end Date	Date	LDAP Server	Attribute: dateendpr7
	Portal Role 8	Pull Down	Web Portal	Hardcoded
	Portal Role 8 start date	Date	LDAP Server	Attribute: datestartpr8
	Portal Role 8 end Date	Date	LDAP Server	Attribute: dateendpr8
	Report Access Level	Drop-down	RD_USERSECURITY	Data_Viewability

DSD 6/Architecture – System Security/Database Entities /Reporting Database Key Relationships

There are no key relationships within security-based reporting database tables.

DSD 6/Architecture – System Security/Business Class Definitions

Security DSD does not have Business Class Definition content.