COLYAR CONSULTING GROUP, INC.

Child Nutrition Programs

Application Support Manual

Colorado Department of Public Health and Environment

For System Administrators
FINAL V1.0

Colyar Consulting Group, Inc. – 22420 N. 18th Dr., Phoenix, AZ 85327 - Phone 623.209.1700 • Fax 623.580.8770

TABLE OF CONTENTS

TABLE OF FIGURES

1

Introduction

Welcome to the Colorado Department of Public Health and Environment (CDPHE) user manual for the Maintenance & Configuration and Security modules. This web-based software solution provides administrators, state users, and Institutions with efficient and immediate access to applications, claims, and related nutrition program functions. This manual provides information on managing the configurations and security of the system. It will be used by authorized state staff that acts as System Administrators.

Web Site Benefits and Features

This system is a user-friendly web application that allows authorized state agency personnel and Institutions to submit and approve application, claims, and miscellaneous forms via the Internet. Key system features include:

- A software system that manages information regarding Institutions, applications, claims, and reports.
- A single integrated database which serves all child nutrition programs.
- The ability to save partially completed forms on-line, allowing the user to complete the process at a later time.
- Individual User IDs and passwords for secure login to program functions and accurate tracking of user behavior.
- A robust security module that streamlines security setting controls by enabling administrators to easily assign users to numerous pre-defined groups and eliminating the need to manually set each user's security access.

User Manual

This user manual is intended for use by authorized system administrators. It is designed to provide a general understanding of how to use the system in an effective and efficient manner. This manual will provide:

- A general explanation of each feature available.
- Screen examples of web site pages and forms.

- Step-by-step instructions for utilizing the web site features.
- Tips and notes to enhance your understanding of the system.

2

Getting Started

Before you can begin using the system's administrative modules, you must be assigned a user ID and password by a System Administrator that provides the required security rights. Once this setup is complete, you may use the Internet and your assigned user ID and password to access and log onto the web site.

Logging On

To log on

1. Access the system by typing the URL into the address line of your web browser of choice
   -OR-
   Open the website from your Desktop or Internet Favorites.

   Note: Please contact CDPHE for the URL web address.

2. In the Log On box, enter your **User ID**.
3. Enter your **Password**.
4. Select **Log On**.

TIP: The Password is case-sensitive, so if your password includes upper and lower-case letters ensure that it is entered correctly.

Note: If you do not have a User ID and Password, contact your System Administrator.

Note: If this is your first time logging on, you will be required to change your password.

To change your password

1. Select a new password and enter it into the box provided.
2. Re-enter your new password for confirmation.
3. Select **Save** to continue to the Programs page.

Programs Page

Once you successfully log on, the Programs page is displayed. Actual access to specific modules is based on the user's security rights. For example, Institution users will not have access to the Accounting, Maintenance and Configuration, and Security modules because these modules are only for authorized State users.

TIP: The Accounting, Maintenance and Configuration, and Security tiles are always gray because these are administrative modules that are available to only authorized State users. Institutions will not have access to these modules.

Note: If your User ID is associated with only one (1) module, the Programs screen will not display; the system will automatically take you to the module you are authorized to access.

Figure 1: Programs Page

Selecting this button…	Provides…
Child and Adult Care Food Program	Access to the Child and Adult Care Food Program home page
Accounting	Access to the Accounting Module home page
Maintenance and Configuration	Access to the Maintenance and Configuration module home page
Security	Access to the Security Module home page

3

Maintenance and Configuration Module

Now that you know how to access and log on to the system, let's focus on the functions of the Maintenance and Configuration module. The Maintenance and Configuration module is used by authorized System Administrators to maintain configurable system functions and tables.

Maintenance and Configuration home page

After logging into the system using your assigned user name and chosen password and selecting the Maintenance and Configuration button, you will be taken to the Maintenance and Configuration module home page.

To access the Maintenance and Configuration home page

1. Log on to the web site.
2. Select the **Maintenance and Configuration** tile. The home page displays.

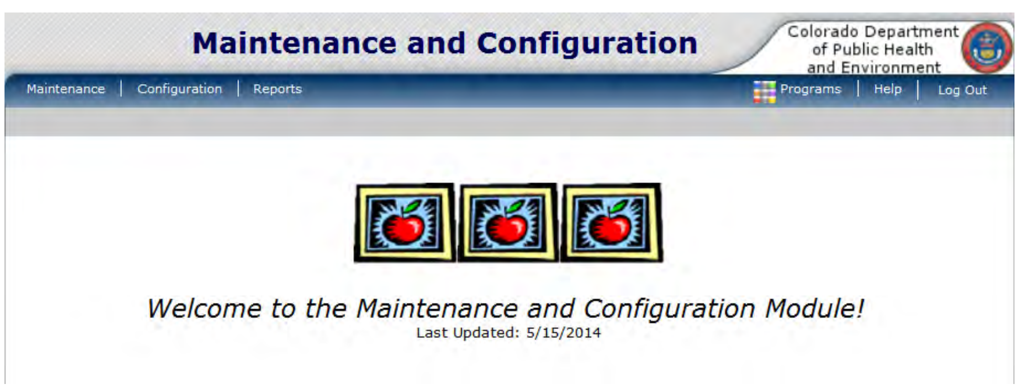


Figure 2: Maintenance and Configuration module home page

The Maintenance and Configuration module menu bar provides access to the Maintenance and Configuration sub-modules. From here, you can select Maintenance or Configuration on the blue menu bar at the top of the page. The following table describes the features available from each menu option. Please note that based on your security level you may not have edit or view access to all screens.

Menu option	Menu Features
Maintenance	Access to overall maintenance items including: ▪ Checklist Maintenance ▪ Claim Rate Maintenance ▪ Counties ▪ Download Forms ▪ Error Codes ▪ Message Board Maintenance ▪ Program Year Maintenance ▪ Recalculate Claims ▪ Rep & Consultant User Maintenance
Configuration	Access to overall system security configuration items including: ▪ User Configuration Settings ▪ Activity Log Settings

Maintenance Menu

The Maintenance Menu is your access point to most functions within the Maintenance and Configuration module.

To access the Maintenance Menu

1. Log on to the web site.
2. Select the **Maintenance and Configuration** tile. The Maintenance and Configuration module home page displays.
3. On the blue menu bar, select **Maintenance** to display the Maintenance Menu.
4. Select the Maintenance function you wish to access.

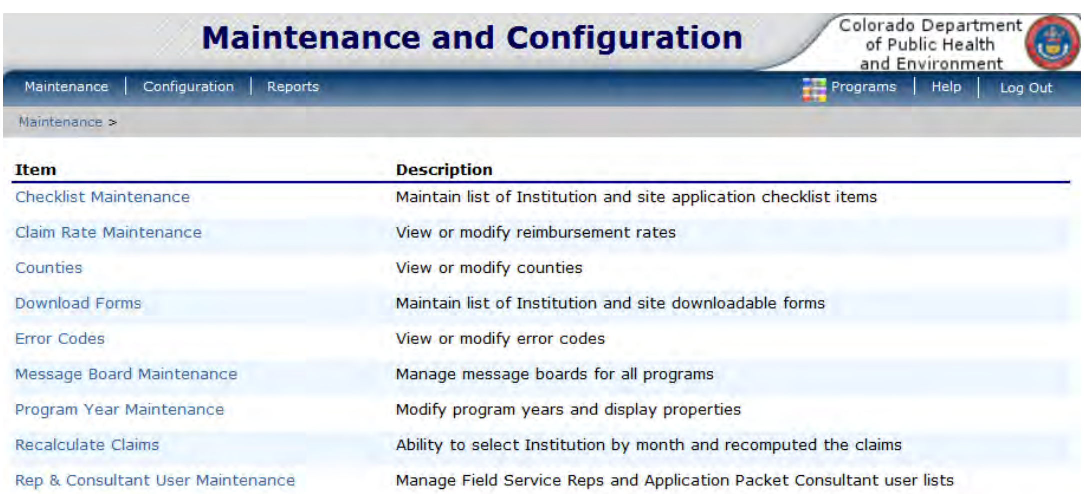


Figure 3: Maintenance Menu

Checklist Maintenance

Checklist items are associated with a Institution's application packet. The system will automatically generate a defined Checklist item on a Institution's checklist based on business rules coded within the software. Post-implementation, State administrators **cannot** add a checklist item without going through the change control process.

Checklist items are loaded into a Institution's checklist based upon answers to specific questions on a Institution's application or particular conditions (e.g., a new Institution). The Checklist Maintenance feature allows authorized administrators to view or modify the start/end date for a specific checklist item and associate a checklist item with a form defined in the system (see ***Download Forms***).

Unlike the Download Forms function, Checklist items are not deleted through a Delete function. Instead, "old" checklist items are given end dates, after which the checklist item will expire and will no longer display to users.

To view or modify a checklist

1. On the Maintenance menu, select **Checklist Maintenance**. The Checklist Maintenance screen displays.

TIP: Selecting the Description, Start Date, End Date or Program column header will sort the data in ascending/descending order.

Checklist Maintenance

Description	Start Date	End Date	Program
Human Services (CCAP) attendance billing forms for the month prior	1/1/2002		CACFP
Child Care Center License	1/1/2002		CACFP
Food Service Management Contract	1/1/2002		CACFP
Fire or Health Inspection	1/1/2002		CACFP
Health Inspection	1/1/2002		CACFP
Copies of completed income eligibility forms classified as free and reduced	1/1/2002		CACFP
Human Services Medicaid Fiscal Agreements	1/1/2002		CACFP
Medicaid Billing Forms for the month prior	1/1/2002		CACFP
Medicaid Survey/Certificate	1/1/2002		CACFP
Pre-Approval Site Visit Form	1/1/2002		CACFP

Figure 4: Checklist Maintenance screen (partial)

2. Select the Checklist item you wish to modify. The Checklist Item screen displays.
3. Enter the Checklist Item name. This is the exact name that appears on the Checklist.
4. If the checklist item is associated with a form maintained within the system in the Download Forms table, select the respective form in the Download Form drop down.

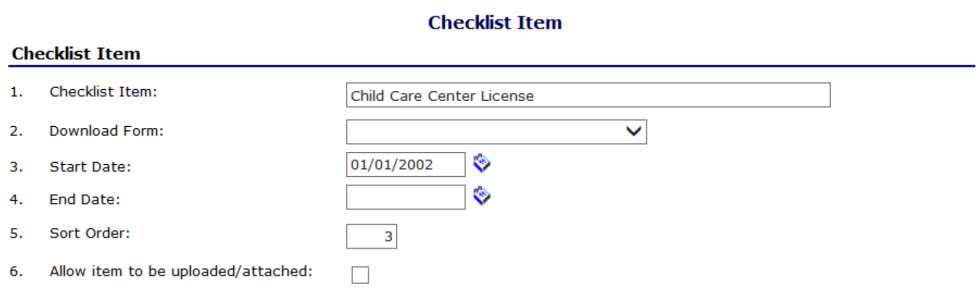
TIP: By associating the checklist item with a form maintained in the system (via the Download Form function), the checklist item becomes a link to the user and they can access the form template from the Checklist screen. The user does not need to access the form from the Download Forms menu item on the Applications menu.

5. Identify the Start Date as to when the checklist item should appear on the Institution's Application Packet checklist and the order of where the checklist item should appear on the checklist.

TIP: If you want a checklist item to expire at a specific time (e.g., end of a specific school year), enter an End Date. After that date, the checklist item will no longer appear to users.

The End Date field is **optional**. If no date is entered, the checklist item will never expire and will always appear if the required condition exists.

6. Make the desired date change and select **Save**.


Checklist Item

Checklist Item

1. Checklist Item: Child Care Center License
2. Download Form:
3. Start Date: 01/01/2002
4. End Date:
5. Sort Order: 3
6. Allow item to be uploaded/attached:

Figure 5: Checklist Item screen

TIP: By selecting the "Allow item to be uploaded/attached" checkbox, the item will have a paperclip next to it on a Institution's Checklist screen. This enables the user to attach a document and load it into the system.

WARNING: To associate a checklist item to a form template stored on the database, you must first define the form in the Download Forms table so that it appears in the Download Forms dropdown on this screen. See ***Download Forms*** section.

Claim Rate Maintenance

The Claim Rate Maintenance function enables authorized State administrators to view or modify reimbursement rates for all programs. Reimbursement rates are entered by program for a specific school year. The system uses these rates to properly calculate amounts earned based on entered claims to determine the correct payment amount for each claim based upon the respective claim period and school year.

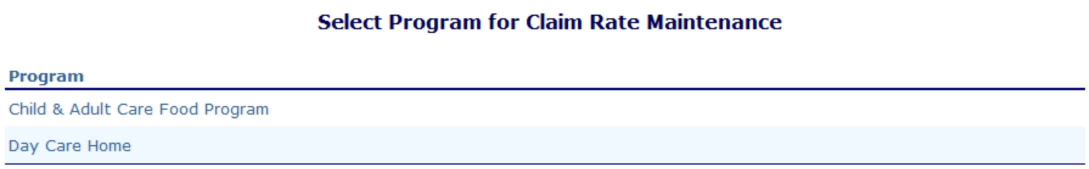


Figure 6: Select Program for Claim Rate Maintenance screen

To modify a claim rate

1. On the Maintenance menu, select **Claim Rate Maintenance**.
2. Select the program with the claim rate you wish to modify.
3. Select the Program Year for which you wish to modify the rates. The Claim Reimbursement Rates for the selected program in the selected year screen displays (see the following figures).
4. Make the desired changes in rates and programs.
5. Select **Save**.

TIP: Selecting the Program Year, Begin Date, or End Date headings will sort the dates in ascending or descending order.

WARNING: Even if claim rates are setup properly, no claims can be processed until the State completes the Grant screens in the Accounting module.

Example: Claim Rates for CACFP

This is an example of the Claim Rates for CACFP screen. Rates will be saved up to the fourth decimal (e.g., entering “2.93” will be saved as “2.9300”). It is not necessary to enter up to the fourth decimal place.

Claim Rates for CACFP

Federal Reimbursement Operating Rates - July 1, 2013 to June 30, 2014

Breakfast

	Maximum Reimbursement
Free	1.5800
Reduced	1.2800
Paid	0.2800

Lunch

	Maximum Reimbursement
Free	2.9300
Reduced	2.5300
Paid	0.2800
CIL	0.2325

Supper

	Maximum Reimbursement
Free	2.9300
Reduced	2.5300
Paid	0.2800
CIL	0.2325

Snack

	Maximum Reimbursement
Free	0.8000
Reduced	0.4000
Paid	0.0700

At Risk Snack

	Maximum Reimbursement
Free	0.8000

At Risk Supper

	Maximum Reimbursement
Free	2.9300

Figure 7: Claim Rates for CACFP screen

Counties

The Counties table identifies the State's counties, respective two digit county code, and rural/urban indicator (as used in the SFSP module).

Counties

Action	Code	Description	Rural / Urban
View | Modify	001	Adams	URBAN
View | Modify	002	Alamosa	URBAN
View | Modify	065	Alt. Agency	URBAN
View | Modify	003	Arapahoe	URBAN
View | Modify	004	Archuleta	URBAN
View | Modify	005	Baca	URBAN
View | Modify	006	Bent	URBAN

Figure 8: Counties screen (partial)

To view or modify a county

1. On the Maintenance menu, select **Counties**.
2. Select the Action (View or Modify) for the county you wish to access.
3. Make the changes desired. You may change the following:
   - County Code
   - County Name
   - Rural/Urban Indicator.
4. Select **Save**.

County

County

Code: 001

Description: Adams

Type: Urban

Figure 9: County screen

Note: On most screens, the County Name and County Code are concatenated to display as County Name (County Code). For example: Adams (001). This is a display feature. To add a new county, enter the County Code and County Name in the respective fields. Do not concatenate the code and name into the County Name field.

Download Forms

The Download Forms function provides the State the ability to identify form templates or external websites that can be accessed from within the system. This eliminates the need for a user to access a separate website to view additional information or access a template or form.

Through this function, the State can save form templates to the system database, which can be downloaded by the Institution through the Applications menu of their selected program or through the Application Packet's Checklist, if the form is associated with a checklist item (see ***Checklist Maintenance***).

Instead of creating a form template, the State may decide to provide direct access to a State website that already maintains these templates. Through the Download Forms function, the State can also associate a form to an associated website URL where the form is located. This eliminates the need for the State to maintain duplicate versions of the same form on to different websites.

To view or modify a form's display properties

1. On the Maintenance menu, select **Download Forms**. The Download Form Group list displays.

Download Forms

Form ID	Description	Last Modified	New Institution?
14	New Sponsor Form	11/17/2011	Y
CACFP-001 CACFP Management Plan	CACFP Management Plan for Centers	08/15/2013	Y

Figure 10: Download Forms screen

> **Note:** The figure above is an example of download forms that may be available for viewing. Current forms available on the system may not match those detailed in the figure.

2. Select the Form ID link for the desired form.
3. Modify the Form details.
4. Select Save.

To view or modify a form's download details

1. From the Download Forms screen, select the Form ID link of the form whose download details you wish to modify. The Download Form screen displays.
2. Select the **EDIT** link.
3. If the form is associated with a URL and not a document, you can modify the form's URL in the File URL field.

   If the form is associated with a document and you would like to replace the document with a newer version or another document, enter the End Date and select Save. Continue to **STEP 2** described in the ***To add a form*** section.
4. Select **Save**.

TIP: When a new version of an existing form has been created and it is necessary to replace it within the database, enter the End Date for the “old” version (i.e., this will ensure the form is not accessible to users).

Then, use the ADD New Detail link on the Download form screen to upload the new form into the database. Remember to enter the Start Date that is applicable for the new form.

If the form is just pointed to a webpage (URL), and there is no start/end date scenario, you can edit the URL.

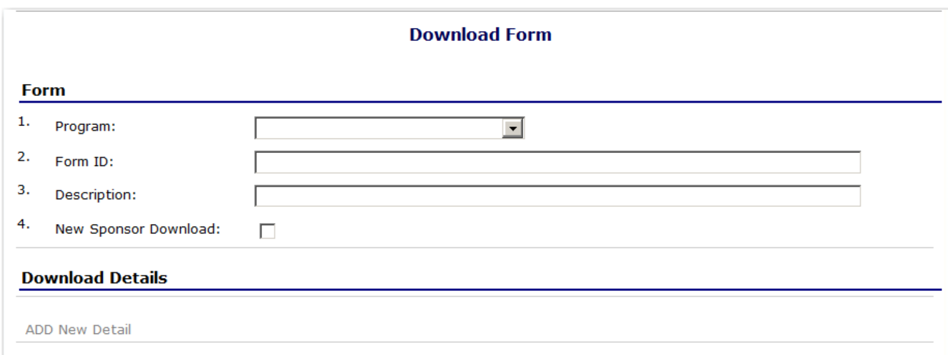
To add a download form to a group

Adding a new form is completed in two steps:

1) Defining the form in the system.
2) Associating the defined form with an actual file that is loaded into the database or an external URL link.

STEP 1: Defining the Form

1. On the Download Forms screen, select **Detail** for the desired group.
2. Select **Add New Downloadable Form to Group**. The Download Form screen displays.


Download Form

Form

1. Program:
2. Form ID:
3. Description:
4. New Sponsor Download:

Download Details

ADD New Detail

Figure 11: Download Form – Add New Downloadable Form screen

3. Select the Program’s menu under which the form can be accessed (e.g., Day Care Home).
4. Enter the Form ID and Description.
5. Select the New Sponsor Download checkbox if the form is applicable to new Institutions. On the Download Forms screen, the form will have a “Y” in the New Institution column.
6. Select **Save**.

STEP 2: Associating the Form to a File or URL

1. Select the **<Edit** button on the confirmation screen to return to the download form screen.
2. Select **ADD New Detail** link. The Download Form Detail screen displays.

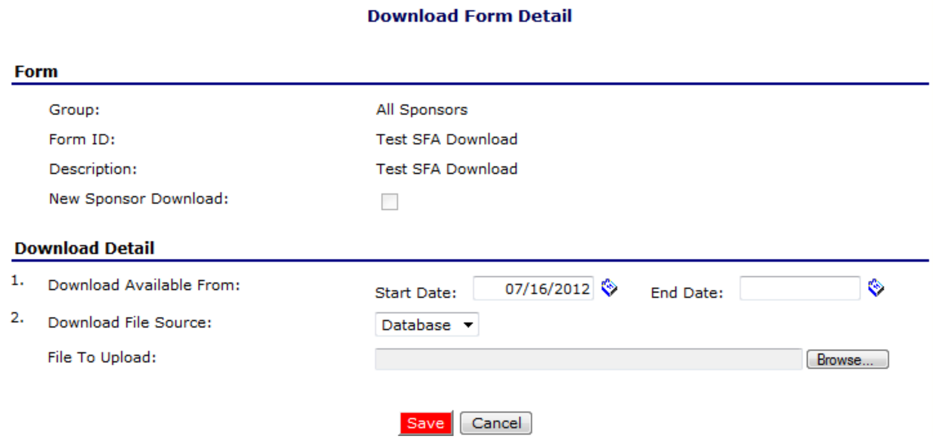


Figure 12: Download Form – Download Detail

3. Enter the Start Date and End Date.

Note: Input dates in the following format: MM/DD/YYYY.

TIP: You may leave the End Date blank if you do not have a defined date when the form should no longer be available to the user. If a form is valid until a certain date (example: a new version of the form will be released on MM/DD/YYYY), you can use the End Date to make the form unavailable to the user on the specified date.

4. Identify whether the Download File Source is the Database (i.e., selecting the form within the system will retrieve the document from the database) or a Website (i.e., selecting the form within the system will open a new window directed at the specified URL).
5. If the Download File Source is the Database:
   - Select the **Browse** button.
   - Your desktop will display the **Choose File to Upload** pop-up.
   - Navigate to the current location of the file you want to upload.
   - Select **Open** from within the pop-up**.**
   - Select **Save**.

   If the Download File Source is a Website:
   - Enter the URL where the form should link to.
   - Select **Save.**

To delete a form

1. On the Maintenance menu, select **Download Forms**. The Download Forms list displays.
2. Select **Details** for the desired group.
3. Select **Modify** for the form you wish to delete. The Download Form screen displays.
4. On the Edit toolbar, select **DELETE**. A warning message displays confirming that you want to perform the delete action.
5. Select the **Delete** button. A confirmation screen displays.
6. Select **Finish** to return to the list of Download Forms.

WARNING: Once the download form has been deleted, it is permanently removed from the system and cannot be restored. It must be re-added. Use caution before deleting a form.

Error Codes

The Error Codes function provides general information for each error code included in the entire system (i.e., for all programs). When an error is triggered by the user on a screen, the Error Code number, Error Description, and Error Code Type are displayed on the top of the screen.

A small set of errors are classified as "client-side" errors and are generated without having to go to the server. These are basic errors such as the data entered is not in the correct format (e.g., letters are entered into numeric only fields). Since these types of errors do not reach the server, the error messages are "canned" messages managed outside the Error Codes table.

The Error Codes table is used to manage "server-side" errors (e.g., relational edits). "Server-side" errors are referenced within the software code. Authorized State administrators would access the Error Codes function **ONLY** to modify the error message displayed to the user and/or modify the error code type.

TIP: Changes the text of an error message in the Test environment will NOT change the error message verbiage in the Production environment. Remember, these are separate databases.

To view or modify an error code

1. On the blue menu bar, select **Maintenance**.
2. On the Maintenance and Configuration menu, select **Error Codes**. The list of all error codes is displayed.

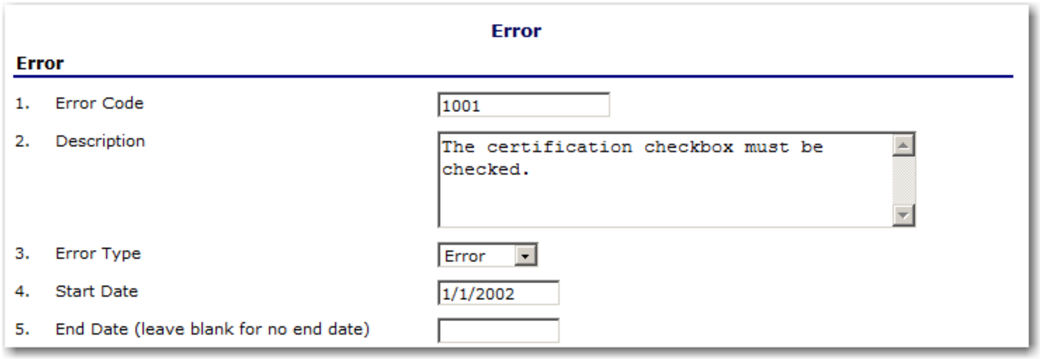
Error Codes

Error Code	Description	Error Type
1001	Certification - The certification checkbox must be checked.	ERROR
1002	School Year Dates of Operation - Start Date is required.	ERROR
1003	School Year Dates of Operation - Start Date must be before End Date.	ERROR
1004	School Year Dates of Operation - Start Date cannot be prior to July 1st of the current school year.	ERROR
1005	School Year Dates of Operation - End Date is required.	ERROR
1006	School Year Dates of Operation - End Date must be after Start Date.	ERROR
1007	School Year Dates of Operation - End Date cannot exceed June 30th of the current school year.	ERROR
1100	Physical Address - Address must be provided. Address Line 2 may be blank.	ERROR

Figure 13: Error Codes screen (partial)

TIP: Selecting the Error Code, Description, or Error Type column header will sort the data in ascending/descending order.

3. Select the error you wish to view/modify. The Error screen displays.



Error

Error

1. Error Code — 1001
2. Description — The certification checkbox must be checked.
3. Error Type — Error
4. Start Date — 1/1/2002
5. End Date (leave blank for no end date)

Figure 14: Error screen

On this screen you can modify:

- Description
- Error Type
- Start Date
- End Date

Note: Input dates in the following format: MM/DD/YYYY.

WARNING: NEVER CHANGE AN ERROR CODE OR THE MEANING OF AN ERROR!

The error code is referenced within the software in order to trigger the correct error message to the user based on the defined business rules. DO NOT make any modifications to an error code. Changing an error code, or the fundamental meaning of an error, will adversely impact the system's error processing function.

4. Select **Save**.

TIP: The End Date field is optional. If no value is entered, the error code will always display if the specified condition is met. Generally, all error codes will have a blank End Date.

TIP: There are two Error Types: Error and Warning. The following table describes these two types of errors:

Error: Prevents the form from being completed. Form cannot be submitted.

Warning: Warns the user of "non-standard" data input. Does not prevent the user from submitting the form.

Message Board Maintenance

The Message Board Maintenance function enables authorized System Administrators to manage the message boards for each module, as well as the message board on the system home (i.e., “splash”) page. Within this function, you can create, modify, and remove messages.

To access Message Board Maintenance

1. On the Maintenance menu, select **Message Board Maintenance.** The Message Board Program List displays.
2. Select the **Program / Module** message board you wish to maintain -OR-
   Select **PUBLIC** to maintain the message board on the system home page.

Message Board Program List

Program / Module	Description
Accounting	Accounting Program
CACFP	Child and Adult Care Food Program
CNFG	Configuration and Maintenance
SCRT	Security Configuration
PUBLIC	Login Screen Message Board

Figure 15: Message Board Program List screen

TIP: The Public message board is viewable on the system home page and therefore accessible to non-users. The message boards for all other modules are viewable only to users with access to that module.

To create a new message board

1. On the Maintenance menu, select **Message Board Maintenance**. The Message Board Program List screen displays.
2. Select the module on which you want to create a new message board. The Message Board List for the selected program/module displays.

Message Board List for CNFG

Heading	Last Updated Date	Display
Configuration Message Board	5/15/2014	(•) Yes ( ) No

Figure 16: Message Board List screen

3. Select **Create New Message Board**. The Message Board screen for the selected program/module displays.
4. Enter the **Message Board ID**. This is internal only and does not display on the screen.
5. Select the **Graphic**. Select **View graphics** to see the list of currently available graphics.
6. Enter the Message Text.
7. Select **Save**.

TIP: Make sure only ONE message board per module has a display set to "Yes".

Example: Message Board for Configuration

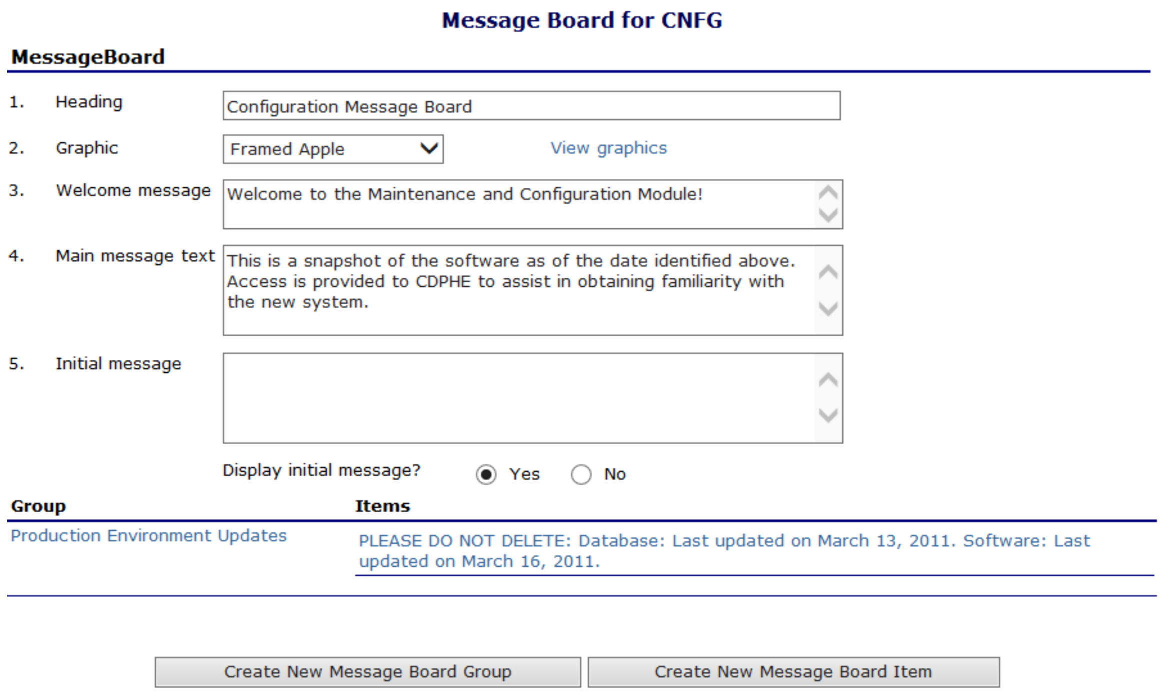


Figure 17: Message Board for Maintenance and Configuration (example)

To create a message board group

TIP: If a message or group of messages relate to a specific topic (e.g., Training) or are targeted toward a specific group or function (e.g., Fresh Fruit and Vegetable Program), the System Administrator may choose to create a message board group. This will create a section on the home page, providing a group heading in bold print to draw the user's attention.

1. On the Maintenance menu, select **Message Board Maintenance**. The Message Board Program List displays.
2. Select the module on which you want to create a new message board group. The Message Board List for the selected module displays.
3. Select name of the desired message board Heading.
4. Select **Create New Message Board Group**. The Message Board Item for the selected program/module displays.
5. Enter the **Text**. This is the name of the message board group as it will appear on the home page (e.g., Training Information). Keep it brief and meaningful.
6. Enter the **Start Date** and **Expiration Date**. These fields are not required. If no dates are entered, the message group will appear on the home page immediately and will remain until an expiration date is entered or the message board group is deleted.

   Note: Input dates in the following format: MM/DD/YYYY.

7. If desired, enter the **Sort Order**. This field is not required. It can be used to manage the display order when you have multiple message board groups

TIP: When there is more than one message board group for a specific program/module, the system will use the sort order to determine the order of display.

8. Select **Save**.

Figure 18: Create New Message Board Group

To create a message board item

WARNING: In order to create a message board item, the message board group under which the item will display must already be defined within the system.

1. On the Maintenance menu, select **Message Board Maintenance**. The Message Board Program List displays.
2. Select the module on which you want to create a new message board group. The Message Board List for the selected module displays.
3. Select name of the desired message board Heading.
4. Select **Create New Message Board Item**. The Message Board Item for the selected program/module displays.

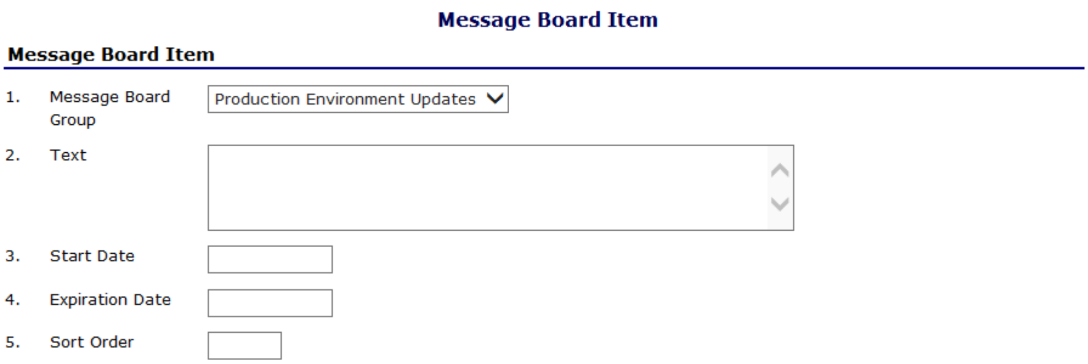


Figure 19: Message Board Item screen (example)

5. Select the **Message Board Group** to which you want to add an item.
6. If desired, enter the **Start Date and Expiration Date**. These fields are not required. If no dates are entered, the message board item will appear on the home page immediately and will remain until an expiration date is entered or the message board item is deleted.

Note: Input dates in the following format: MM/DD/YYYY.

7. Enter the **Sort Order**. This field is not required. It can be used to manage the display order when you have multiple message board items in a single message board group.

TIP: When there is more than one message board item for a specific message board group, the system will use the sort order to determine the order of display on the home.

8. Enter the **Text**. This is the message to appear on the screen.
9. Select **Save**.

To delete a message board

1. On the Maintenance menu, select **Message Board Maintenance**. The Message Board Program List displays.
2. Select the program/module for the message board you want to access. The Message Board List for the selected program/module displays.

3. Select **DELETE** on the Edit toolbar in the top-right corner. A warning message displays confirming that you want to perform the delete action.
4. Select the **Delete** button.

WARNING: Selecting the button permanently deletes the message board and any related items (e.g., message board groups and items). It will not be recoverable once deleted. Use caution before deleting message boards.

To delete a message board group

1. On the Maintenance menu, select **Message Board Maintenance**. The Message Board Program List displays.
2. Select the program/module you want to access. The Message Board List for the selected program/module displays.
3. Select the the Group you wish to delete.
4. Select **DELETE** on the Edit toolbar in the top-right corner. A warning message displays confirming that you want to perform the delete action.
5. Select the **Delete** button.

WARNING: Selecting the button permanently deletes the message board group and it will not be recoverable once deleted.

Figure 20: Message Board Group - Delete (example)

To delete a message board item

1. On the Maintenance menu, select **Message Board Maintenance**. The Message Board Program List displays.
2. Select the program/module you want to access. The Message Board List for the selected program/module displays.
3. Select the Item you wish to delete.
4. Select **DELETE** on the Edit toolbar in the top-right corner. A warning message displays confirming that you want to perform the delete action.

5. Select the **Delete** button.

WARNING: Selecting the button permanently deletes the message board item and it will not be recoverable once deleted.

Program Year Maintenance

Program Year Maintenance enables authorized administrators to modify the accessibility to data by program year. This is used to manage whether the applications and/or claims functions are opened, closed, or view-only for Institution and/or state users.

The following table describes the options:

Item	Description
Open	Data can be accessed for the respective program year and can be modified
View	Data can accessed for the respective program year, but can only be viewed
Closed	Data cannot be accessed for the respective program year

Selecting **Program Year Maintenance** from the Maintenance Menu displays the Select Program for Year Maintenance list.

Figure 21: Program Year Maintenance and Configuration screen

Note: This function drives the years accessible via the School Year link at the top of all screens. As soon as the program year ends, the respective year should be put in "View" mode. By setting the year to "Closed", it will not appear in the School Year page.

Generally, three (3) years of data are made accessible to Institutions and five (5) years of data are made accessible to State users. For program years greater than these years, set all displays to "Closed". This will remove the program year from all related menus and reduce screen clutter.

To view or modify a program year

1. On the Maintenance menu, select **Program Year Maintenance**.
2. Select the Program you wish to modify.
3. Select the Program Year you wish to modify.
4. Make the desired modifications and select **Save**.

To create a new program year

1. On the Maintenance menu, select **Program Year Maintenance**.
   The Select Program for Year Maintenance and Configuration screen displays.
2. Select the Program you wish to modify.
3. Select **Create New Program Year**. A new program year screen displays.
4. Enter the Begin Date and End Date into the available text boxes.
5. Using the drop-down option, select whether the applications and claims functions are open, view-only, or closed for Institutions (i.e., Institutions) displays.
6. Using the drop-down option, select whether the applications and claims functions are open, view-only, or closed for State employees displays.
7. If desired, select the check-box at the bottom of the screen to display the “New” image on the application year select list screen.

> **TIP:** Select the checkbox next to the “**Show the ‘New’ image on the application year select list screen**” to alert users that a new year has been created. This image does not disappear until the check box is deselected. When selecting this image for a new year, be sure that the previous year's image is disabled.

8. Select **Save** once all information has been entered.

Example: Child and Adult Care Food Program

This is an example of the Program Year Maintenance screen for CACFP.

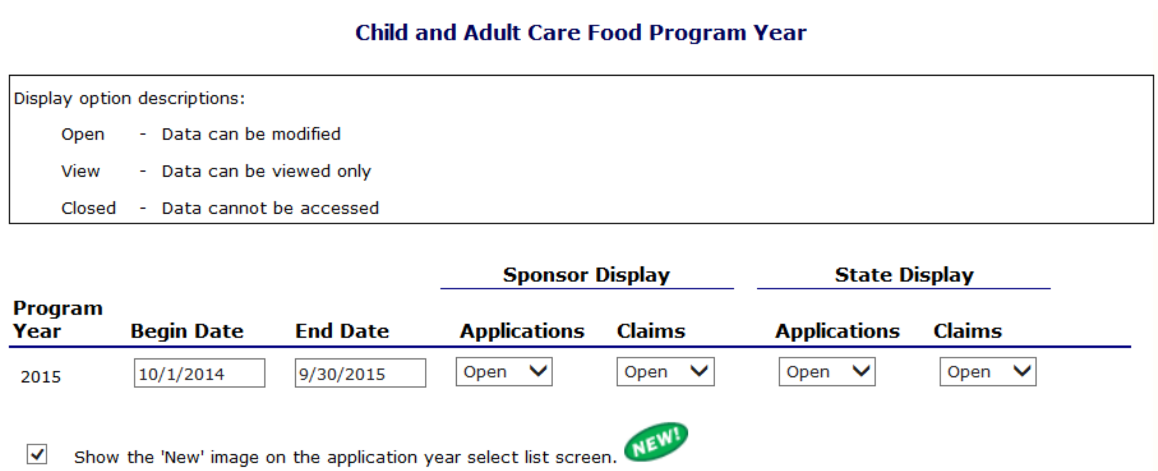


Figure 22: Child and Adult Care Food Programs Year screen

Rep & Consultant User Maintenance

The Rep and Consultant User Maintenance function provides the ability to identify State users who serve as representatives or consultants to the Institutions. Once a user is defined as a representative or consultant, their name will appear in the respective dropdown fields on the Search, Institution Profile, and Assignment screens.

The system allows for three (3) types:

- **Application Packet Consultant**: Individuals responsible for reviewing and approving Application Packets. Used by the Application submodule for CACFP.
- **Field Service Rep**: Individuals assigned in the field to support the Institution. Used by the Compliance sub-module.
- **Specialist**: Individuals who serve as a point of contact regarding program-related concerns. Informational; not used by any module.

Note: Most States do not use all these types.

To view or modify assigned Representatives and Consultants

1. On the Maintenance screen, select **Rep & Consultant User Maintenance**. The Rep & Consultants menu displays.

Rep & Consultants

Name
Application Packet Consultant
Field Service Rep
Specialist

Figure 23: Rep & Consultants screen

2. Select the type of representative or consultant you would like to view or modify.
3. The Rep & Consultant Users screen displays a list of users associated with the selected group.

Rep & Consultant Users

Name: Application Packet Consultant

List Filter

Show users participating in : ALL Apply Filter

First Name	Last Name	CACFP	Status
State	User	N	Active
SCN	Tester (Brad)	Y	Active
SCN	Tester (Jennifer)	Y	Active

Figure 24: Rep & Consultants Users screen

TIP: The default is to display a list of all users associated with the selected group. To narrow available users by program, use the drop-down box in the List Filter to choose the program for which you would like to view available users. For example, if you only want to see only users supporting SNP, select **SNP** from the drop-down box and Select **Apply Filter.**

4. To view the details of a specific user, select the name of the representative/consultant. The Rep & Consultant User Detail screen displays.
5. Make desired modifications and select **Save**.

Figure 25: Rep & Consultants User Detail screen

To add a Representative or Consultant

1. On the Maintenance menu, select **Rep & Consultant User Maintenance.** The Rep & Consultants menu displays.
2. Select the type of representative or consultant you would like to add. The Rep & Consultant Users screen displays a list of users associated with the selected group.
3. Select **Add User**. The Rep & Consultant User Detail screen displays.
4. Select the user you would like to add from the **Users (State Employees)** drop-down list.
   - The drop-down list displays all users that are identified in the Security module's User Profile Screen as "State employees".
5. Select the program(s) the user is associated with and therefore would appear in the applicable screens within the respective modules.
6. Select the Status of the user. The system defaults to "Active"
7. Select **Save**.

TIP: The Users Dropdown list lists all State Employees defined in the Security module.

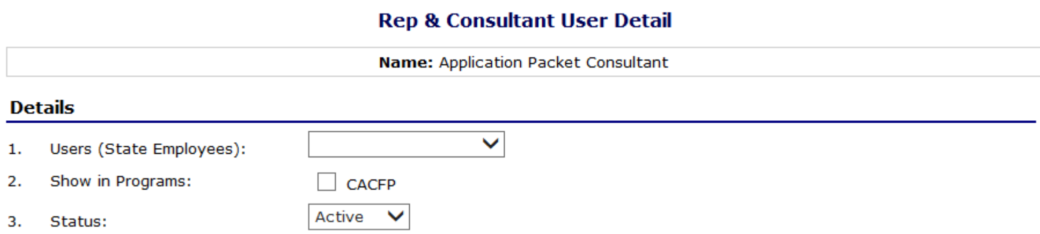


Figure 26: Rep & Consultants User Detail (Add New)

To delete a Representative or Consultant

1. On the Maintenance screen, select **Rep & Consultant User Maintenance**. The Rep & Consultants menu displays.
2. Select the type of representative or consultant you would like to delete. The Rep & Consultant Users screen displays a list of users associated with the selected group.
3. Select the name of the representative/consultant you would like to delete. The Rep & Consultant User Detail screen displays.
4. Select **DELETE** on the Edit toolbar in the top-right corner. A warning displays.
5. Select the **Delete** button.

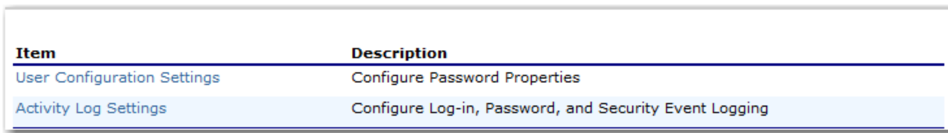
WARNING: Once a user has been deleted, it is permanently removed from the Rep & Consultants section and will no longer be associated to any Institutions. The User's security account will remain active within the system. Use caution before deleting Rep & Consultant users.

Configuration Menu

The Configuration sub-module provides authorized State System Administrators the ability to configure and maintain system-wide security module settings related to log in, password, and security event logging.

To access the Configuration Menu

1. Log on to the web site.
2. Select the **Maintenance and Configuration** tile. The Maintenance and Configuration module home page displays.
3. On the blue menu bar, select **Configuration** to display the Configuration Menu.
4. Select the Configuration function you wish to access.



Item	Description
User Configuration Settings	Configure Password Properties
Activity Log Settings	Configure Log-in, Password, and Security Event Logging

Figure 27: Configuration Menu

Once you access the Configuration menu, you can select the feature you wish to access. The following table describes the options available on the Configuration menu:

Menu option	Description
User Configuration Settings	View or modify system-wide security properties for State and Non-State Employees.
Activity Log Settings	View or modify security activity log settings for log ins/outs, password changes, and security changes.

User Configuration Settings

This feature enables authorized administrators to view and modify system-wide security properties for State and Non-State Employees.

To view or modify the user configuration settings

1. On the Configuration menu, select **User Configuration Settings**. The User Configuration Settings screen displays.
2. Make any desired changes and select **Save**.

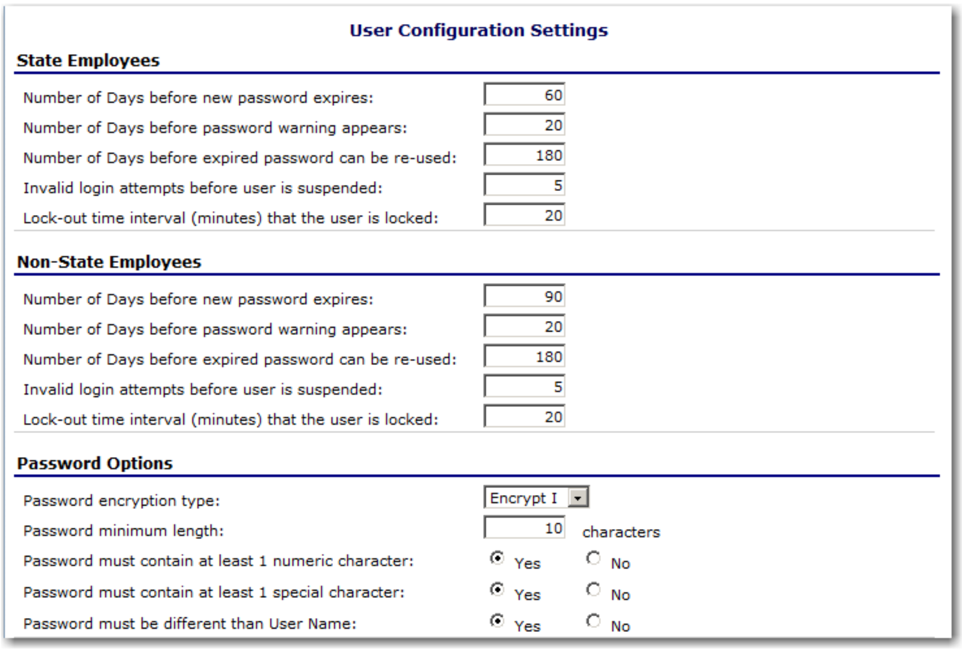


Figure 28: User Configuration Settings screen

Activity Log Settings

This feature enables authorized System Administrators to view or modify security activity log settings for log ins/outs, password changes, and security changes.

To view or modify the activity log settings

1. On the Configuration menu, select **Activity Log Settings**. The Activity Log Settings screen displays.
2. Make the desired changes and select **Save**.

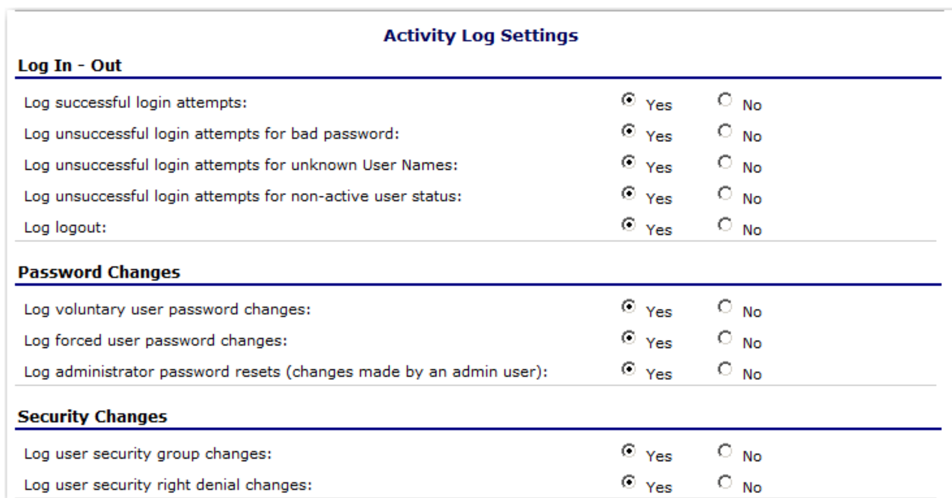


Figure 29: Activity Log Settings screen

Refer to ***Security Reports*** section for instructions on accessing activity logs.

Reports

The Maintenance and Configuration module has the capability to accommodate maintenance-related reports. At this time, no standard reports are provided in the system.

4

Security Module

This section of the manual will focus on the functions of the Security module. Within the Security module, System Administrators can define and configure user and group profiles and related security rights.

Security module home page

After logging on to the system, authorized users will be able to access the Security button on the Programs screen. Selecting the Security button will take you to the Security module home page. This page contains the Security message board.

Note: The message board for the Security module is maintained within the Maintenance and Configuration module. For more information about updating and maintaining message boards, please see the ***Maintenance and Configuration*** section of this manual.

To access the Security module home page

1. Log on to the system using your user ID and password.
2. Select the **Security** tile. The Security module home page displays.

Note: If you are already logged on and need to return to the Programs menu, select **Programs** on the blue menu bar at the top of the page. Then, select **Security.**

From the Security module home page, you can use the Security module menu bar at the top of the page to select the **Security** or **Reports** menu. The following table describes the features available from each menu option.

Menu option	Menu Features
Security	▪ **User Manager:** Enables state users to create new users, maintain User's Profiles, change/reset passwords, set assigned groups, and manage security rights and associated Institutions. ▪ **Group Manager:** Enables state users to create new groups, manage group security rights, and maintain group profiles.
Reports	▪ **Report List:** Contains reports available within the Security module.

TIP: If at any time, you wish to access a different module within the system, just select **Programs** in the blue menu bar and select the program you wish to access.

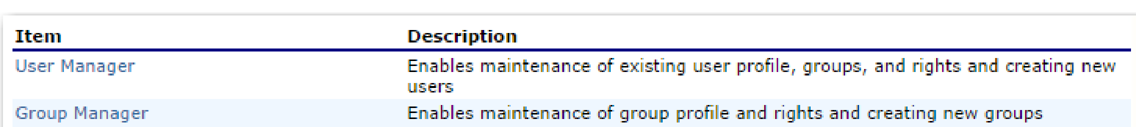
The remainder of this manual will discuss each menu item of the Security module. Please note that based on your security level, you may not have edit or view access to all screens.

Security Menu

The Security menu screen provides authorized users with the functionality to maintain user information via the User Manager screen and security group information via the Group Manager screen. The User Manager enables authorized administrators to create new users, update User's Profiles, manage security rights, and reset passwords. The Group Manager enables authorized administrators to create new groups, update group profiles, and maintain group rights.

To access the Security menu

1. On the blue menu bar at the top of the page, select **Security**
2. Select the security function you wish to access.



Item	Description
User Manager	Enables maintenance of existing user profile, groups, and rights and creating new users
Group Manager	Enables maintenance of group profile and rights and creating new groups

Figure 30: Security Menu

User Manager

The User Manager allows you to set up and maintain various components of a user's security access. This feature enables authorized administrators to add new users, maintain User's Profiles, change passwords, and set assigned groups, security rights and associated Institutions.

To access User Manager

1. On the blue menu bar at the top of the page, select **Security**.
2. Select **User Manager**. The Search for User screen displays.

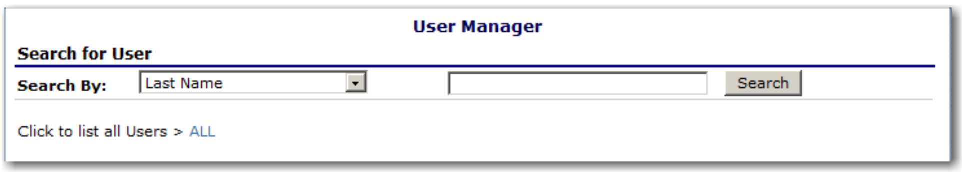


Figure 31: Search for User Page

To search for a user

Before proceeding in the User Manager, you must search for and select a user to manage. If you have already selected a user or are elsewhere in the application, return to the User Manager screen.

1. On the User Manager screen, select the type of search on the **Search By** drop-down list (Last Name or User Name) and select **Search**.
   —OR—
   Select **All** to display a list of all users.
   A list of users matching the search criteria displays.

> **Note:** State Employees are listed in Bold. Security Administrators are indicated by "Yes" in the Administrator column. Not all State Employees are Security Administrators.

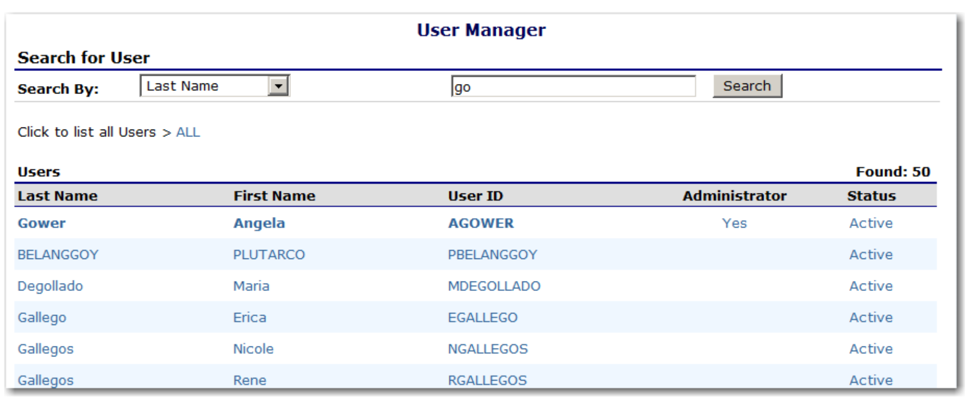


Figure 32: User Manager Search Results (example)

2. Select the user you wish to access. The User Options menu displays.

> **Note:** The menu options displayed on the User Options menu depends on whether the user can access all Agencies (i.e., a State user) or if the user is an Agency user.

User Options

User Name: stateuser **Name:** State User

Item	Description
User's Profile	Specific information for the User.
User's Assigned Group(s)	Security Groups assigned to the User.
User's Security Rights	Security settings for the User.
Reset User's Password	Reset the User's password.

Figure 33: User Options menu - State User (example)

User Options

User Name: Sponsor **Name:** Sponsor CCG

Item	Description
User's Profile	Specific information for the User.
User's Assigned Group(s)	Security Groups assigned to the User.
User's Security Rights	Security settings for the User.
User's Associated SFAs	Associated SFAs for the User.
Reset User's Password	Reset the User's password.

Figure 34: User Options menu - Institution User (example)

To add a new user

If you have already selected a user or are elsewhere in the application, return to the User Manager screen.

1. From the User Manager screen, select **Add New User**. The User's Profile screen displays.

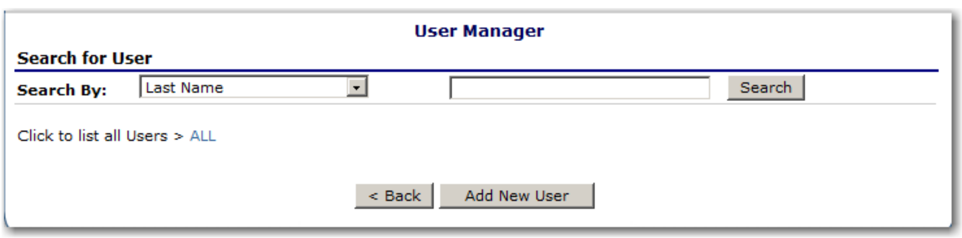


Figure 35: User Manager – Add New User

2. Enter the new user's information in the User Information section. The First Name, Last Name, and Title are required.

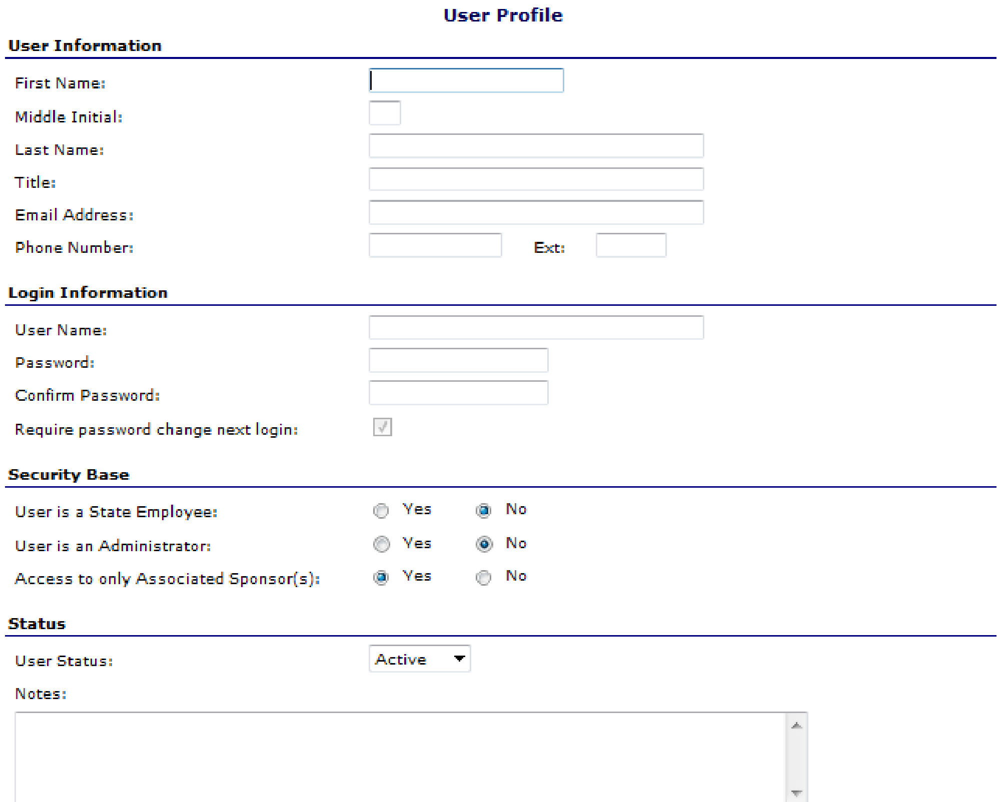


Figure 36: User Profile screen

3. Enter the new user's login name and temporary password. Enter the temporary password again for confirmation. This information is required. The system will prompt the user to change the temporary password upon initial login.

4. Use the buttons to select if the user is a: a) state employee, b) security administrator, and c) granted access to associated Institutions.

> **Note**: If the 'Access to only Associated Institution(s)' button is marked 'Yes', the user will only be able to view information for the Institution(s) to whom they are associated. See also: ***User's Associated Institutions***.

5. Use the drop-down menu to select the user's status. The default is "Active".

6. Select **Save**.

7. Select **<Edit** to return to the User's Profile screen you just modified.
   -OR-
   Select **Finish** to return to the User Options menu.

> **Note**: After creating a new user, it is recommended that you immediately assign the user to a security group. Until the user is linked to a security group, he or she does not have any security rights and will not be able to access any system functions. See also: ***User's Assigned Group(s)***.

User’s Profile

The User’s Profile enables authorized administrators to view and modify a user's basic information, login, security base, and status. In addition to name, contact, and login information, the user's profile specifies whether the user is a: a) state employee, b) security administrator, and c) granted access to associated Institutions. These specifications affect which program functions the user may access.

Furthermore, users specified as **Active** have access to all normal functions, while **Inactive** and **Locked** users are not permitted to login or access the system.

Note: Passwords cannot be changed within the user's profile. This function is accessed through the User Manager. See ***Reset User's Password***.

Note: This screen displays in MODIFY mode by default. To view only, select **VIEW** in the Edit menu (top-right corner).

To access User’s Profile

1. On the blue menu bar, select **Security**.
2. Select **User Manager**. The Search for User screen displays.
3. On the **Search By** drop-down list, select the type of search and then select **Search**.
   —OR—
   Select **All** to display a list of all users.
   A list of users matching the search criteria displays.
4. Select the user you wish to access. The User Options menu displays.
5. Select **User’s Profile**. The User’s Profile screen displays.

To view or modify a user’s profile

1. Access the User’s Profile you wish to view or modify through the User Manager.
2. Modify any desired information.
3. Select **Save**.
4. Select **<Edit** to return to the User’s Profile screen you just modified.
   -OR-
   Select **Finish** to return to the User Options menu.

To delete a user’s profile

1. Access the User’s Profile you wish to delete through the User Manager.
2. On the Edit menu, select **DELETE**. A warning displays at the bottom of the page.
3. Select **Delete**. A confirmation screen displays.
4. Select **Finish** to return to the User Options menu.

WARNING: It is HIGHLY recommended that User Profiles are NOT deleted since data updates have most likely meet "stamped" with the user information. Instead, set the User Profile Status to Inactive.

WARNING: Once a profile has been deleted, it cannot be restored and the User ID assigned to that profile **cannot** be re-used. Use caution before deleting profiles. It is preferred to set the status of the User ID to "Inactive" for a period of time prior to deleting a User ID.

User's Assigned Group(s)

The User's Assigned Group(s) feature streamlines security setting controls by enabling you to assign users to numerous pre-defined security groups. Users assigned to a specific security group automatically inherit the security rights defined for the group, eliminating the need to manually set each user's security access.

Any changes to a group's security rights settings will affect any users associated with the security group. In order for existing users to experience security rights setting changes, the user must re-login to the system. Users cannot modify their own assigned groups.

Note: Once a user is assigned to a group, the User inherits the rights defined for the security at the point in time the association is made. To customize a user's rights, see ***User's Security Rights***.

To access User Assigned Group(s)

1. On the blue menu bar, select **Security**.
2. Select **User Manager**. The Search for User screen displays.
3. On the **Search By** drop-down list, select the type of search and then select **Search**.
   —OR—
   Select **All** to display a list of all users.
   A list of users matching the search criteria displays.
4. Select the user you wish to access. The User Options menu displays.
5. Select **User's Assigned Group(s)**. The User's Assigned Group(s) screen displays.

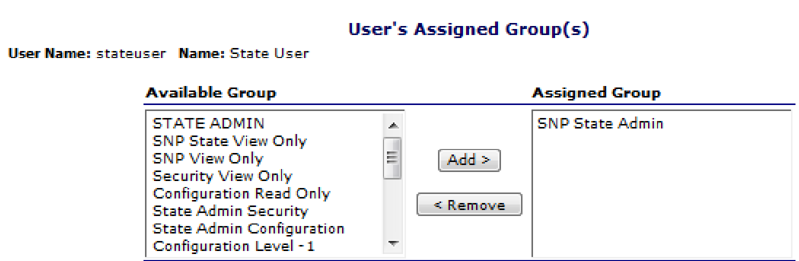
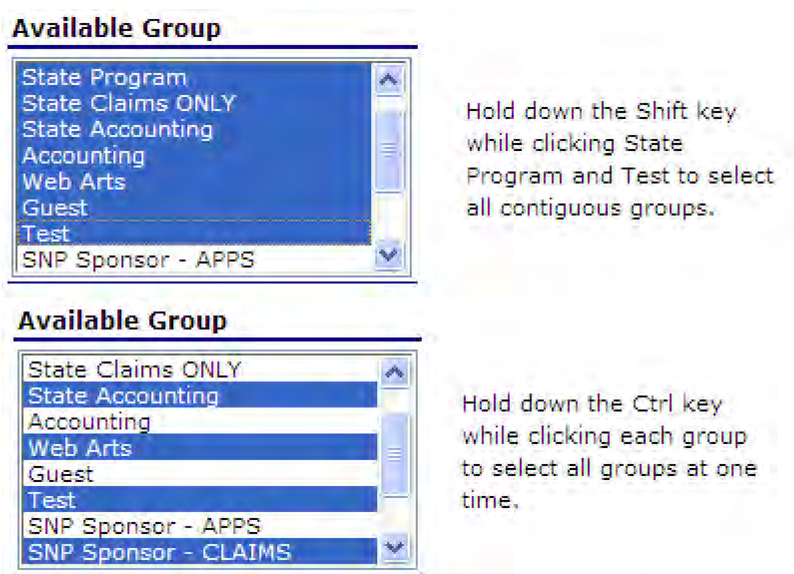


Figure 37: User's Assigned Group(s) Screen

To assign a user to a defined security group(s)

1. On the blue menu bar, select **Security**.
2. Select **User Manager**. The Search for User screen displays.
3. On the **Search By** drop-down list, select the type of search and then select **Search**.
   —OR—
   Select **All** to display a list of all users.
   A list of users matching the search criteria displays.
4. Select the user you wish to access. The User Options menu displays.
5. Select **User's Assigned Group(s)**. The User's Assigned Group(s) screen displays.
6. Select the group you want to add the user to from the **Available Group** list.
7. Select **Add>**. A message box appears and reads "Select 'Save' to Apply the Changes"
8. Select **OK** on the Message box.

TIP: You can easily select multiple groups two ways:



9. Select **Save**.
10. Select **<Edit** to return to the User Assigned Group(s) screen you just modified.
    —OR—
    Select **Finish** to return to the User Options menu.

To remove a user from assigned group(s)

1. On the blue menu bar, select **Security**.
2. Select **User Manager**. The Search for User screen displays.
3. On the **Search By** drop-down list, select the type of search and then select **Search**.
   —OR—
   Select **All** to display a list of all users.
   A list of users matching the search criteria displays.
4. Select the user you wish to access. The User Options menu displays.
5. Select **User's Assigned Group(s)**. The User's Assigned Group(s) screen displays.
6. Select the group you want to remove the user from on the Assigned Group list.
7. Select **<Remove**. A message box appears and reads "Select 'Save' to Apply the Changes"
8. Select **OK** on the Message box.
9. Select **Save**.
10. Select **<Edit** to return to the User's Assigned Group(s) screen you just modified.
    —OR—
    Select **Finish** to return to the User Options menu.

User’s Security Rights

When a user is assigned to a security group, the group’s default security settings will apply and display in the User's Security Rights. No more rights may be given to the user than are given to the group. However, state administrators may deny a user's specific rights.

The User Security Rights feature enables state administrators to customize security rights automatically assigned to an individual user based upon the security group(s) to which they are associated. Security rights determine the functions and actions within the system's programs and modules the user is granted access.

Note: Users cannot modify their own security rights.

To access User Security Rights

1. On the blue menu bar, select **Security**.
2. Select **User Manager**. The Search for User screen displays.
3. On the **Search By** drop-down list, select the type of search and then select **Search**.
   —OR—
   Select **All** to display a list of all users.
   A list of users matching the search criteria displays.
4. Select the user you wish to access. The User Options menu displays.
5. Select **User’s Security Rights**. The User’s Security Rights screen displays.

33

Figure 38: User Security Rights Screen (partial)

To modify User’s Security Rights

1. On the blue menu bar, select **Security**.
2. Select **User Manager**. The Search for User screen displays.
3. On the **Search By** drop-down list, select the type of search and then select **Search**.
   —OR—
   Select **All** to display a list of all users.
   A list of users matching the search criteria displays.
4. Select the user you wish to access. The User Options menu displays.
5. Select **User’s Security Rights**. The User’s Security Rights by Program screen displays.
6. Select the applicable **Program**.
7. Modify the desired information.
8. Select **Save**.
9. Select **<Edit** to return to the User Security Rights screen you just modified.
   —OR—
   Select **Finish** to return to the User Options menu.

> **Note**: The security rights available to a user depend on the User’s Assigned Group(s). Only the security rights assigned to the User’s Assigned Group(s) display in the user's security rights.
>
> If you wish to assign additional security rights to a user that are not displayed as options in the user's security rights, you will need to assign the user to the security group with the desired rights and then customize the user’s security rights.

User’s Associated Institutions

In order for Institution users to have access to system functions for a Institution, users must be associated with the Institution. The User's Associated Institutions feature enables authorized administrators to associate users to specific Institution(s). Most Institution users are associated with only one Institution; however, there are some Institution users that are associated with more than one Institution.

The User’s Associated Institutions function provides the ability to associate one or more Institutions to a User ID.

To access User’s Associated Institutions

1. On the blue menu bar, select **Security**.
2. Select **User Manager**. The Search for User screen displays.
3. On the **Search By** drop-down list, select the type of search and then select **Search**.
   —OR—
   Select **All** to display a list of all users.
   A list of users matching the search criteria displays.
4. Select the user you wish to access. The User Options menu displays.
5. Select **User’s Associated Institutions**. The User’s Associated Institutions screen displays.

To add a Institution association

8. On the blue menu bar, select **Security**.
9. Select **User Manager**. The Search for User screen displays.
10. On the **Search By** drop-down list, select the type of search and then select **Search**.
    —OR—
    Select **All** to display a list of all users.

    A list of users matching the search criteria displays.
11. Select the user you wish to access. The User Options menu displays.
12. Select **User’s Associated Institutions**. The User’s Associated Institutions screen displays.
13. Select **Add Institutions**. The Add User’s Associated Institutions screen displays.

User's Associated Sponsors

User Name: vabell **Name:** Vicki Abell

Associated Sponsors

Actions	Sponsor	Sponsor Name
Remove	11269	Just For Kids

Figure 39: Add User’s Associated Institutions Screen

14. Enter the **Agreement Number** or the **Institution Name**, and then select **Search**.
    —OR—
    Select **All** to display a list of all Institutions.

A list of Institutions matching the search criteria displays.

8. Select **Add Association** to the left of the Institution you want to associate with the user.
9. Select **Finish**. The User's Associated Institution screen displays with the newly added Institution on the list.

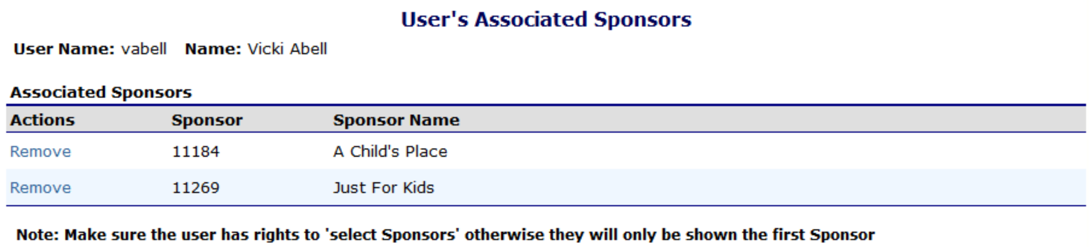


Figure 40: User's Associated Institutions screen (partial)

To remove a Institution association

1. On the blue menu bar, select **Security**.
2. Select **User Manager**. The Search for User screen displays.
3. On the Search By drop-down list, select the type of search and then select Search.
   —OR—
   Select **All** to display a list of all users.
4. A list of users matching the search criteria display.
5. Select the user you wish to access. The User Options menu displays.
6. Select **User's Associated Institutions**. The User's Associated Institutions screen displays.
7. Select **Remove** to the left of the Institution you want to remove. A confirmation message displays.
8. Select **Finish**. The User's Associated Institution screen displays with the Associated Institution no longer on the list.

Reset User's Password

The Reset User's Password enables authorized security administrators to reset a user's password required to login to the system.

Note: Passwords can be reset for users who have forgotten their passwords. If a user attempts to log in with an incorrect password, a login error will display. Only five unsuccessful login attempts are permitted before the user is temporarily locked out of the system. The number of unsuccessful login attempts can be modified through the Maintenance and Configuration module.

Remember, passwords are case-sensitive!

To access Reset User's Password

1. On the blue menu bar, select **Security**.
2. Select **User Manager**. The Search for User screen displays.
3. On the Search By drop-down list, select the type of search and then select Search.
   —OR—
   Select **All** to display a list of all users.
4. A list of users matching the search criteria displays.
5. Select the user you wish to access. The User Options menu displays.
6. Select **Reset User's Password**. The Reset User's Password screen displays.

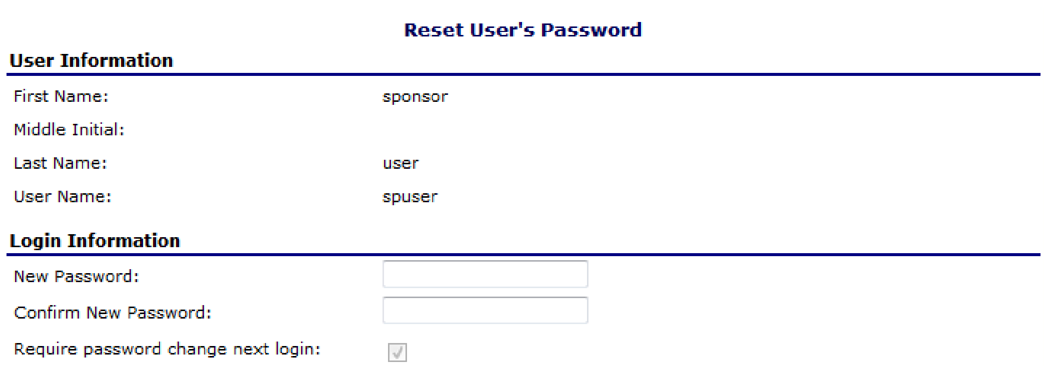


Figure 41: Reset User's Password Screen

To reset a User's Password

1. On the blue menu bar, select **Security**.
2. Select **User Manager**.
   The Search for User screen displays.
3. On the **Search By** drop-down list, select the type of search and then select **Search**.
   —OR—
   Select **All** to display a list of all users.

   A list of users matching the search criteria displays.
4. Select the user you wish to access. The User Options menu displays.
5. Select **Reset User's Password**. The Reset User's Password screen displays.
6. Enter the **New Password**. This is the temporary password.
7. Re-enter the temporary password in the **Confirm the New Password** field.

   Note: The **Require password change next login** check box cannot be modified. This feature's purpose is to inform the individual that the user will need to change their password upon their next login.
8. Select **Save**.
9. Select **<Edit** to return to the Reset User's Password screen.
   —OR—
   Select **Finish** to return to the User Options menu.

Group Manager

The Group Manager function allows you to set up the user rights for a Security Group. All users assigned to that group will have the same access rights to the programs. For example, a Institution group would not have access to accounting functions (since accounting features are for state users only), while the administrator group would have access to all functions.

The Group Manager is the portal to add new security groups, modify group profiles and security rights, and delete group profiles.

To access Group Manager

1. On the blue menu bar, select **Security**. The Security menu displays.
2. Select **Group Manager**. The Security Groups list displays.

Security Groups

Security Group
STATE ADMIN
CACFP Sponsor Admin
DCH Sponsor Admin
CACFP Sponsor Claims
DCH Sponsor Claims
CNP System Group

Figure 42: Security Groups Screen

3. Select the Security Group you want to view or modify. The Security Group Options menu displays.

Security Group Options

Security Group: State User

Item	Description
Group's Profile	Defines security properties for the group.
Group's Security Rights	Defines associated security rights for the group.

Figure 43: Security Group Options Screen

To add a new group

1. On the blue menu bar, select **Security**. The Security menu displays.
2. Select **Group Manager**. The Security Groups list displays.
3. Below the list of existing groups, there is an **Add New Group** button. Select the **Add New Group** button. The Security Group Profile screen displays.

Security Group Profile

Security Group Information	
1. Group Name:	CACFP Sponsor Admin
2. Parent Group:	
3. State Employees only:	☐
4. Display Order:	99

Figure 44: Security Group Profile Screen

4. Enter the **Group Name**.
5. Select the **Parent Group**.

> **Note:** If a parent group is selected from the drop-down list, the new group will display underneath the selected parent group. This option may be left blank.

> **WARNING:** The child group security rights will inherit the rights of the parent AT THE TIME the child group was created. Subsequent changes to the parent group will not change the existing child group.

6. Select whether the group is **State Employees only**. This selection impacts user functionality (e.g., access to the INTERNAL USE ONLY link, ability to view all Institutions in the system, etc.).
7. Enter the **Display Order** on the Security Group screen. This identifies the display sort order of the new group on the Security Groups screen.

> **Note:** A number must be entered for the display order. If the new group shares a display order number with an existing group, the groups will display on the Security Groups list alphabetically.

8. Select **Save**. Select **<Edit** to return to the Security Group Profile screen you just modified.
   —OR—
   Select **Finish** to return to the Security Group Options menu.

To view or modify a group’s profile

1. On the blue menu bar, select **Security**. The Security menu displays.
2. Select **Group Manager**. The Security Groups list displays.
3. Select the Security Group you want to view or modify. The Security Group Options menu displays.
4. Select **Group’s Profile**. The Security Group Profile menu displays.
5. Enter the desired changes.
6. Select **Save**.
7. Select **<Edit** to return to the Security Group Profile screen you just modified.
   —OR—
   Select **Finish** to return to the Security Group Options menu.

To delete a group’s profile

1. On the blue menu bar, select **Security**. The Security menu displays.
2. Select **Group Manager**. The Security Groups list displays.
3. Select the Security Group you want to view or modify. The Security Group Options menu displays.
4. Select **Group’s Profile**. The Security Group Profile menu displays.
5. On the Edit menu, select **DELETE**. A warning displays.
6. Select **Delete**. A confirmation screen displays.
7. Select **Finish** to return to the Security Group Options menu.

WARNING: Once a group’s profile has been deleted, it cannot be restored and any related items will be removed with the profile. Use caution before deleting profiles. The system will not allow the deletion of a group if users are associated with the group.

To view or modify a group’s security rights

1. On the blue menu bar at the top of the page, select **Programs**.
2. Select **Security**.
3. On the blue menu bar, select **Security**. The Security menu displays.
4. Select **Group Manager**. The Security Groups list displays.
5. Select the Security Group you want to view or modify. The Security Group Options menu displays.
6. Select **Group’s Security Rights**. The Group's Security Rights screen displays.
7. Make any desired modifications.
8. Select **Save**.

9. Select **<Edit** to return to the Group Security Rights screen you just modified.
—OR—
Select **Finish** to return to the Security Group Options menu.

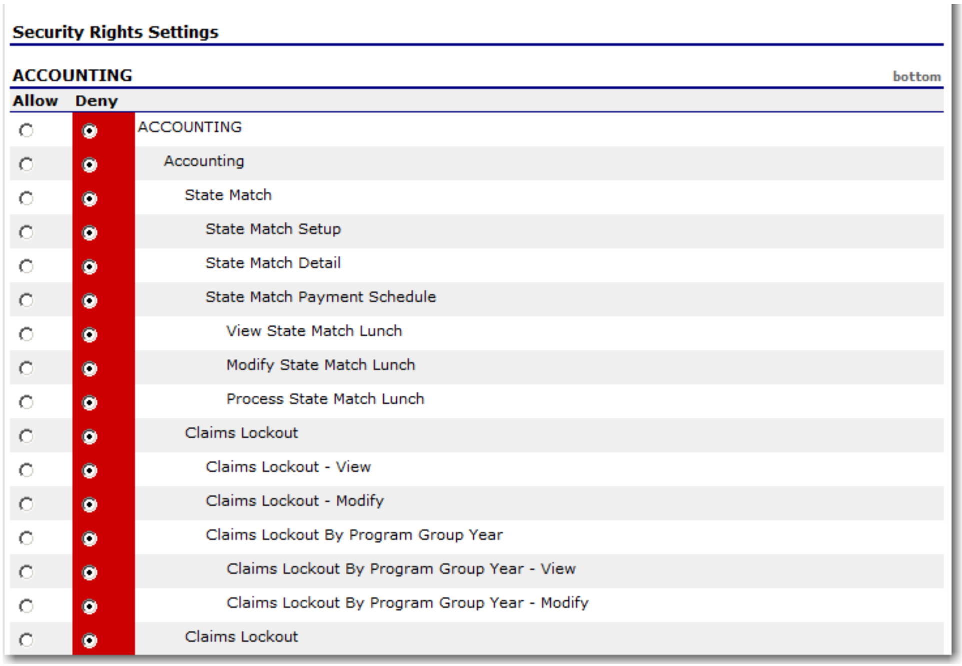


Figure 45: Group Security Rights Screen (partial)

Reports

The Reports function of the Security module enables authorized security administrators to generate, view and print security-related reports.

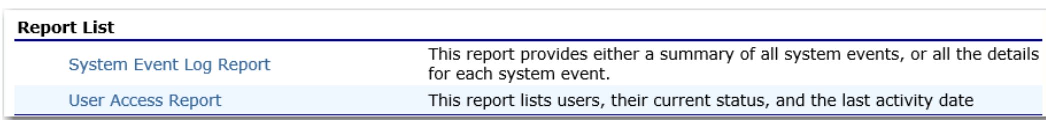
To view report

1. On the blue menu bar at the top of the page, select **Reports**. The Report List displays.
2. Select the report you wish to view from the Report List. The report parameters screen may display.
3. If required, use the drop-down lists and/or text fields to enter parameters.
4. Select Create Report. The report displays in a new window in HTML format.

WARNING: The report will not open in a new window if you have a pop-up blocker running on your system. Either turn off pop-up blocker or hold down the **CTRL** key and select **Create Report** again.

Security Reports

The System Event Log Report provides summary and detail logs regarding security activities.



Report List

System Event Log Report	This report provides either a summary of all system events, or all the details for each system event.
User Access Report	This report lists users, their current status, and the last activity date

Figure 46: Security Reports

Selecting report parameters

Most reports require one or more parameters to be entered allowing the report to be customized to user's specific needs. Report parameters may limit data contained in the report or control how the information is sorted or grouped. Below is an example of report parameters that may be used for running a report.

Figure 47: System Log Report - Report Parameters

Security Reports Examples

There are 3 types of security reports:

1) ***Security Log Summary Report***: This report lists a summary of security events for the date range provided.

2) ***Security Log Detail Report:*** This report lists details of every security-related event for the date range provided.

3) ***User Access Report:.*** This report lists security-related details of each user defined within the system. This report opens directly into Microsoft Excel due to the significant number of data columns.

Event	Occurrence
User login failure, password supplied is incorrect.	18
User has logged in successfully.	161
User has logged out.	110
User's password has been reset.	2
User's password has been reset by an administrating user.	2
User's password has been reset (required).	6
User's security group assignment has changed.	18

Figure 48: Security Log Summary Report (example)

Date	Time	Event Log	Event By	For User/Sponsor
3/7/2012	2:40:40 PM	Login failure - password entered 'CNIPS2012!' is incorrect for User ID 'kfalder'.		kfalder
3/7/2012	2:41:06 PM	Login failure - password entered 'CNIPS2012!' is incorrect for User ID 'kfalder'.		kfalder
3/7/2012	2:56:12 PM	Login failure - password entered 'password4u' is incorrect for User ID 'preed'.		preed
3/7/2012	3:14:14 PM	Login failure - password entered 'CNIPS2012' is incorrect for User ID 'kfalder'.		kfalder
3/7/2012	3:14:25 PM	Login failure - password entered 'CNIPS2012' is incorrect for User ID 'kfalder'.		kfalder
3/8/2012	5:00:49 PM	Login failure - password entered 'Password4u!' is incorrect for User ID 'bbesaw'.		bbesaw

Figure 49: Security Log Detail Report (example)

Last Name	First Name	MI	Title	Email Address	Phone Number	Phone Ext	User Name	Status
Agency	FDP		Agency Test				fdpagency	Active
ANDERSON	GAY		Authorized Rep.		(605) 582-2049		GAYANDERSON	Active
ANDERSON	SHELLY		Authorized Rep.		(605) 862-8108		SHELLYANDERSON	Active
Arbach	Amy		Food Service	amy.arbach@k12.sd.us	(605) 948-2252		AmyArbach	Active
Archambault	Allison		Food Service	allisonarchambault1976@yahoo.com	(605) 823-4971		AllisonArchambault	Active

Figure 50: User Access Report (example – partial view)

5

Security Groups and Guidelines

Security groups are defined and configured by authorized State System Administrators. When new users are added to the system, or a user changes his/her business role, the System Administrator will use the information in this section to determine the optimal security groups to be assigned to the user.

Efficiently Managing Security Groups

The goal is to balance the number of security groups created with the number of security groups needed to efficiently manage the security environment. The system provides features that help with this:

- User-specific customizations.
  - All user IDs associated to a defined security group inherit the rights of the security group. If a small subset of users assigned to a group require a modification from the default security group rights, whether the addition or removal of rights, the System Administrator may customize a specific user ID's rights.
- Multiple Security Groups.
  - A user can be associated with multiple security groups. When the user is assigned to multiple security groups, all the rights are combined for the user to yield the maximum rights allowed by the assigned groups.
- Inherited properties.
  - Defined security groups can be associated with a parent security group. The System Administrator can then customize the rights of the child security group, reducing the amount of work involved in creating security groups.
  - NOTE: By default, the "child" security group will inherit the rights of its parent at the time that the child security group was created. If the parent's rights <u>change</u> after creation of the child security group, the child does not automatically inherit the new rights.

Customizing a User's Security Rights

Once a user is associated with a defined security group, their User ID will automatically inherit the rights associated with the security group. If a user, or small subset of users, should be assigned only some of the inherited security rights, the systems administrator should customize the individual user's security rights as opposed to creating a new security group. To customize a user's inherited security rights, see ***Security Module: User Manager***.

Inheriting Security Groups Rights

To associate a new security group to a parent security group, the System Administrator must define the “parent” security group first. This includes creating the “parent” security group and defining its rights. Once this has been saved, the System Administrator can define a new security group and associate it to the “parent” security group by selecting the correct **Parent Group** on the Security Group Profile screen. For additional information on defining a new security group, see ***Security Module: Group Manager***.

Figure 51: Security Group Profile screen (example)

The following represents how this “child” security group will display on the Security Groups screen.

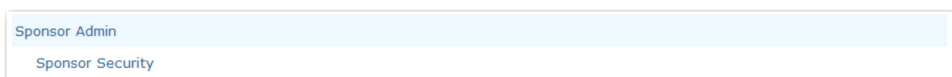


Figure 52: Security Groups screen (parent/child example)

6

Setting Up a New Program Year

Prior to the start of a new program year, authorized state System Administrators must prepare the system for the new year. This section describes the steps to be taken to establish a new program year within the system. All screens referenced in these steps are located in the Maintenance and Configuration module (Maintenance sub-module).

Steps to Establishing a New Program Year

There are five (5) steps required to establish a new program year within CNP:

1. Create the year using the ***Program Year Maintenance*** screen.
2. Define the year's claim rates using the ***Claim Rate Maintenance*** screen.
3. If applicable, define the year's accounting information using the ***Account Codes Maintenance*** screen, as applicable.
4. Update Program Bulletin Boards using the ***Message Board Maintenance*** screen.

WARNING: All of these areas **SHOULD** be defined within the system prior to making a new program year available to users. Failure to do may result in system errors.

Define New Program Year

The first step in configuring the environment for a new program year is to define the new program year within the system. This is completed through the Maintenance and Configuration module. The Program Year Maintenance screen enables authorized administrators to modify the accessibility to data by program year. This is used to determine whether the applications and/or claims functions are opened, closed, or view-only for Institution and/or state users.

WARNING: The first year that should be made available to Institutions is 2014-2015 for Applications and Claims.

Program Year Maintenance enables authorized administrators to modify the accessibility to data by program year. This is used to manage whether the applications and/or claims functions are opened, closed, or view-only for Institution and/or state users.

The following table describes the options:

Item	Description
Open	▪ Data can be accessed for the respective program year and can be modified
View	▪ Data can be accessed for the respective program year, but can only be viewed
Closed	▪ Data cannot be accessed for the respective program year

To create a new program year

1. From the Programs screen, select the **Maintenance and Configuration** module.
2. Select the **Maintenance** menu.
3. Select **Program Year Maintenance.**
4. Select the program you would like to define a new program year.
5. Follows the instructions provided in the ***Program Year Maintenance*** section of this manual.

Note: This drives the program year's accessibility via the Program Year link at the top of all screens. By setting the year to "Closed", it will not appear on the Program Year page.

Define Claim Rates

The system uses claim rates defined in the system to properly calculate payments. These must be defined as part of establishing the new program year.

To define claim rates

1. From the Programs screen, select the **Maintenance and Configuration** module.
2. Select the **Maintenance** menu.
3. Select **Claim Rate Maintenance.**
4. Select the program year you would like to enter claim rates.
5. The Claim Rate Maintenance screen displays.
6. Follows the instructions provided in the ***Claim Rate Maintenance*** section of this manual.

WARNING: Even if claim rates are setup properly, no claims can be processed until the State completes the Grant screens in the Accounting module.

Define Account Codes

For several states, the system relies on the account codes to be defined in order to properly create payments transactions for use in the export file. At this time, this has not be defined for this State.

Establish Message Board Messages

When the program year for a specific program commences, the State usually posts a message on the respective program's message board to call the Institution's attention to specific information. The Message Board Maintenance function enables authorized System Administrators to manage the message boards for all programs.

The most common message posted by States at the start of a new program year is the reminder that the program's application is open for the new year (e.g., 2015-16), and therefore the default Program Year is now the upcoming year; however, claiming continues for the current year (e.g., 2014-15) and therefore the Institution must change the Program Year when entering claims in the current year.

To create a new message board

1. From the Programs screen, select the **Maintenance and Configuration** module.
2. Select the **Maintenance** menu.
3. Select **Message Board Maintenance**. The Message Board Program List screen displays.
4. Select the module's message board to update.
5. Follows the instructions provided in the ***Message Board Maintenance*** section of this manual.