**Common Security Module (CSM)**

User Provisioning Tool (UPT)
User Guide

Version No: 2.0

Last Modified: 11/20/2006

Author   :        Eric Copen, JJ Maurer, Vijay Parmar, Steve Hunter,
Kunal Mod

Team    :        Common Security Module (CSM)

Purchase Order# 34552

Client   :        National Cancer Institute – Center for Bioinformatics,

National Institutes of Health,

US Department of Health and Human Services

# Document History

## Document Location

The most current version of this document is located on the CSM website: http://ncicb.nci.nih.gov/core/CSM

### Revision History

| Version Number | Revision Date | Author | Summary of Changes |
|---|---|---|---|
| 0.1 | 2/7/2005 | Eric Copen | Initial draft |
| 0.2 | 2/9/2005 | Eric Copen | Complete draft |
| 0.3 | 2/15/2005 | JJ Maurer | Review and editorials |
| 1.0 | 2/16/2005 | Eric Copen | Final changes |
| 1.1 | 3/22/2005 | Eric Copen, Jill Hadfield | Formatting, grammar, aesthetic changes, etc. |
| 1.2 | 6/07/2005 | Eric Copen | Update for 3.0.1 release |
| 1.3 | 6/22/2005 | Eric Copen | Update for 3.0.1 release |
| 1.4 | 7/8/2005 | Eric Copen | Changes in response to Jill's review |
| 1.5 | 8/23/2005 | Eric Copen | Removed Standard Negative Privilege language |
| 1.5a | 3/15/2006 | Steve Hunter | Added confirm password field for User |
| 1.5b | 3/17/2006 | Kunal Modi | Added details for lockout information |
| 2.0 | 3/27/2006 | Kunal Modi | Baselined |
| 2.1 | 10/25/2006 | Vijay Parmar | Update for 3.2 release. Added several enhancement descriptions. |

### Review

| Name | Team/Role | Version | Date Reviewed | Reviewer Comments |
|---|---|---|---|---|
| Vinay Kumar | Team Lead | 0.2 | 2/14/05 | Approved |
| JJ Maurer | Ekagra Management | 0.2 | 2/15/05 | Approved with minor changes |
| Jill Hadfield | Technical Writer | 1.0 | 3/14/05 – 3/22/05 | Approved with minor changes |
| Jill Hadfield | Technical Writer | 1.3 | 7/7/05 | Approved with minor changes |
| Kunal Modi | Team Lead | 1.5a | 3/15/2006 | Approved |
| Steve Hunter | QA Engineer | 1.5b | 3/20/2006 | Approved & Baselined |

### Related Documents

More information can be found in the following related CSM documents:

| Document Name |
|---|
| CSM Guide for Application Developers |
| Software Architecture Document |
| CSM Enterprise Architect Model |

**Ekagra**
High Impact – High Value – Business Results

NCICB

| CSM Reference Implementation Guide |
| --- |

These and other documents can be found on the CSM website: http://ncicb.nci.nih.gov/core/CSM

# Table of Contents

# UPT Deployment Guide

## Introduction

The User Provisioning Tool (UPT), part of the overall Common Security Module (CSM) developed for NCICB, is a web application used to configure an application's authorization data. (For more about CSM, refer to the *CSM Guide for Application Developers*, which can be downloaded from http://ncicb.nci.nih.gov/core/CSM) The UPT provides functionality to create authorization data elements like Roles, Protection Elements, Users, etc., and also provides functionality to associate them with each other. The runtime API can then use this authorization data to authorize user actions.

This guide's intended audience is all users of the UPT, including Super Administrators who may add applications and associated administrators, and Administrators who will perform provisioning for a particular application. This guide provides an overview of the application, outlines a suggested workflow, and explains how to perform all UPT operations.

## Workflow

The UPT includes two modes – Super Admin and Admin. The Super Admin operations are typically performed first, as they register the application and application administrators. The primary mode operations, including authorization user provisioning, occur next.

### Super Admin

When first deploying the UPT for a particular application, the developer registers the application in the Super Admin mode. (For details, refer to the *CSM Guide for Application Developers*. Deployment details can be found in the *Provisioning* subsection of the *Deployment Models* section.)

Once the application is registered, the Super Admin can add users who will serve as application administrators. The Super Admin can also register additional applications as they become available. This document details these steps in the *Super Admin Workflow* section.

### Admin

The primary mode is for performing user provisioning for a particular application. The Admin mode follows a simple workflow of creating elements, assigning them, and then associating them. This document details these steps in the *Admin Workflow* section.

## Login

The Login page includes summary text, **What's New**, **Did You Know**, and most importantly the Login section itself: **Login ID**, **Password**, and **Application Name**. For a majority of UPT implementations, the NCICB LDAP serves as the authentication mechanism. Therefore the user's Login ID will be the same as the user's NCICB user name (in Figure 1 and Figure 2, user Eric Copen's NCICB user name is *copene*). Similarly, the Password will equal the NCICB password. The rules from the authentication system are applied to the user name and password.

If logging on as Super Admin, enter the Application Name *csmupt* (see Figure 1). If logging in as an Admin, enter the appropriate application name. For Example **Security** is used in Figure 2.
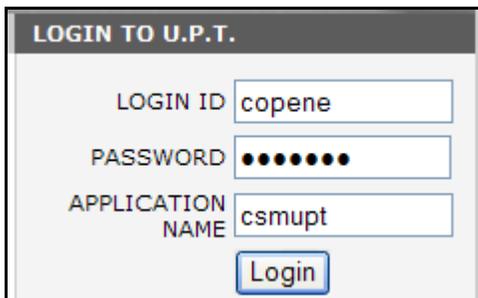
Figure 1 *Login as a Super Admin*
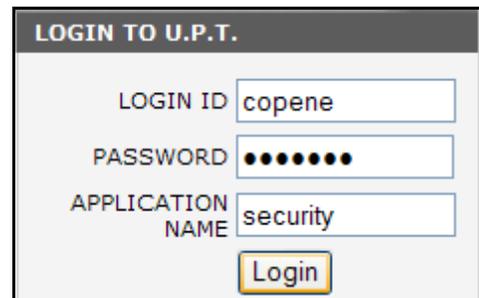
Figure 2 *Login as an Admin*

Since UPT uses CSM's Authentication Manager, it can be configured to lock a user out if they try to make an unauthorized entry into the UPT. If configured appropriately, UPT can lock the user out after a pre-configured number of unsuccessful attempts have been reached in the allowed login time frame. Once locked out, the user can log in only after the configured amount of lockout time has elapsed. This provides security from hacking attempts to break into the UPT.

## Common Basic Functions

Within the UPT, there are several common operations that are repeated for most elements. These operations include **Create New**, **Search** and **Update**, **Delete**, and **Assign/Associate**. This section describes how these operations are performed, and provides screen shots to aid with explanation.

### Create New

When creating a new element follow the steps outlined below. The same basic steps can be followed to create any element; in this example a User is created.

**Step 1:** On the element Home page select **Create a New**…(Figure 3)

**USER LINKS**

Create a New User
Click to add a new user.

Select an Existing User
Enter search criteria to find the user you wish
to operate on.
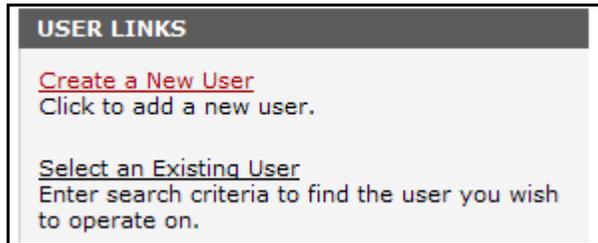
*Figure 3 New and Existing User options*

**Step 2:** Enter details (Figure 4):
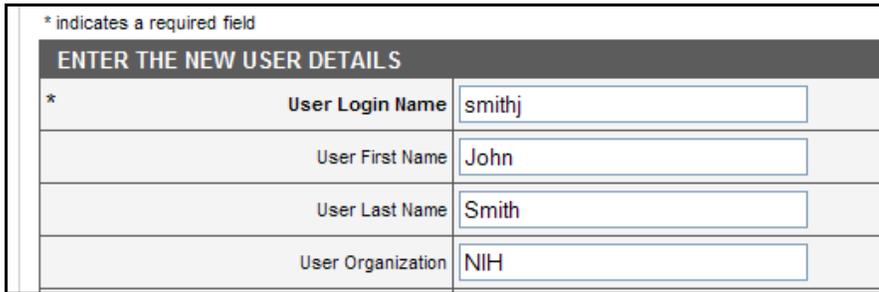


* indicates a required field

**ENTER THE NEW USER DETAILS**

| * | User Login Name | smithj |
| | User First Name | John |
| | User Last Name | Smith |
| | User Organization | NIH |

*Figure 4 Entering new user details*

**Step 3:** Select **Add** to save the new element (in this case User) to the database. This save occurs immediately. **Back** acts exactly like the back button in a browser – returning the user to the home page. **Reset** clears the data from the entire form. Remember that no data is saved until the **Add** button is selected.

**Step 4:** Upon a successful save, the system displays **Add Successful** just below the menu and before the text. In addition, a new set of buttons appears below the details table in Admin mode (Figure 5).



| | Back | Update | Delete |

| Associated Groups | Associated PE & Privileges | Associated PG & Roles | Assign PG & Roles |

*Figure 5 A new set of buttons appear below the menu after you have successfully added a new user. Note: the additional set of buttons is visible in Admin mode only.*

**Example Error Messages:**

The User Interface performs basic data validation, including field lengths and formats. Figure 6 is an example of a message displayed when a user enters an improperly formatted email address:



ERROR
User Email Id is an invalid e-mail address.

*Figure 6 Error message after entering incorrect email address*

The system displays the message in Figure 7 (or similar) if a user tries to add an entry (e.g. *smithj*) when it already exists in the system:

ERROR
An error occured in creating the User. Duplicate entry was found in the database for the entered data

*Figure 7 Error message after entering a user already in the system*

## Search for and Select Existing Elements

When searching for and selecting an element follow the steps outlined below.  The same basic steps can be followed for any element; in this example, a Role is searched for and selected.

**Step 1:** On the element Home page select **Select an Existing…**(Figure 8).

**ROLE LINKS**

Create a New Role
Click to add a new role.

Select an Existing Role
Enter search criteria to find the role you wish to operate on.

*Figure 8 Selecting an existing Role*

**Step 2:** Enter search criteria.  Use the * character to perform wildcard searches (see Figure 9).  For example, searching for Role* returns Role_name_1, Role_name_2, or any other role beginning with role.  A search of *1 returns anything ending with 1 – Role_name_1, Role_name_101, Role_name_51, etc.  **Select Search** for results.  **Back** returns the user to the home page.  **Reset** clears the data.

ENTER THE ROLE SEARCH CRITERIA

Role Name  *1

[Back]  [Search]  [Reset]

*Figure 9 Entering search criteria for Role*

**Step 3:** The system returns a list of matching roles. The results are sorted alphabetically for all search result screens. (Figure 10):

| SEARCH RESULTS | | |
| --- | --- | --- |
| Select | Role Name | Role Description |
| ○ | Role_name_1 | Role_Desc_1 |
| ○ | Role_name_101 | Role_Desc_10 |
| ○ | Role_name_51 | Role_Desc_5 |

*Figure 10 Role search results*

**Step 4:** Select the desired element, in this case **Role_name_1**, by clicking on the radio button in the **Select** column (Figure 11).  You can select one element at a time to view.

| ⊙ | Role_name_1 | Role_Desc_1 |
|---|---|---|

*Figure 11 Example of selecting an element with a radio button*

**Step 5:** Click on the **View Details** button below the Search Results table:

The system then displays this element's details.  (See the following section, *Update*.)

**Example Error Messages:** If the search criteria results in no matches, the system displays an error indicating there are no matches in a search.  Modify the search criteria and repeat until the intended results appear.

## Update

When updating an element follow these steps.  The same basic steps can be followed for any element; in this example, a Protection Element is updated.

**Step 1:** Reach the details screen.  There are two ways to reach the details screen – either create a new element (See *Create New*) or search for and select an existing element (See *Search for and Select Existing Elements*).  The details screen (Figures 12 and 13) displays information such as name and description:

**PROTECTION ELEMENT DETAILS**

| * | Protection Element Name | Test PE Name1103749550261 |
|---|---|---|
| | Protection Element Description | Test Desc |

*Figure 12 Protection element details*

**Step 2:** Simply replace existing text, and select **Update**.

**PROTECTION ELEMENT DETAILS**

| * | Protection Element Name | Test PE Name1103749550261 |
|---|---|---|
| | Protection Element Description | This is my new text I want to update. |

*Figure 13 Entering text for a Protection Element*

**Step 3:** Upon a successful update, the system displays **Update Successful** just below the menu and before the text.

**Example Error Messages:** The User Interface performs basic data validation, including field lengths and formats.  The systems also check for duplicates; it prevents changing the element name to one that already exists.  See the *Example Error Messages* section for more detail.

## Delete

When deleting an element, follow these steps.  The same basic steps can be followed for any element; in this example, a Group is deleted.

**Step 1:** Reach the Group Details screen.  From the home page, either create a new Group (see *Create New*) or search for and select an existing Group (see *Search for and Select Existing Elements*).  The element's Details screen displays a button containing the text Delete.

**Step 2:** Click on the button titled **Delete**.

**Step 3:** A pop-up window asks **Are you sure you want to delete the record?.**  Click **Okay** to confirm.  Clicking **Cancel** negates the operation and returns the display to the Details screen.

**Step 4:** Upon confirming the deletion, the system returns you to the Group home page and displays in blue text the words, **Delete Successful**.

## Assignments and Associations

The elements Role, Protection Group, and Group are simply collections of other elements – Privileges, Protection Elements, and Users respectively.  Provisioning includes assigning elements to elements or removing elements from an element (we call this *deassign*).  For example, assigning Users to Groups greatly improves the ease by which one can provision access rights.  An Admin can instantly assign a role and protection group to an entire group of people instead of repeating the same assignment for each individual.

**Assign or Deassign Privileges, Roles, ProtectionGroups, Groups**:

**Step 1:** Navigate to the Association screen.  From the element home page, either create a new element (see *Create New*) or search for and select an existing element (see *Search for and Select Existing Elements*).  The element's Details screen displays a button containing the text **Associated**, **Assign**, or something similar depending on the element type.

**Step 2:** With this UI implementation, associations can be established or removed by simply selecting elements and moving them from one box to another.  The box on the top lists the Available Groups (unassigned) and the box below lists the Groups assigned to the User – Group_Northeast, Group_ProjectLead, and Group_Research_A.  Simply highlight a Group and select **Assign** to move it to the Assigned Groups box.  Select **Deassign** to move it back to the Available Groups box.

There are multiple ways to highlight the elements within the box:

1.   Select one by clicking on the user name entry.

Ekagra

High Impact – High Value – Business Results

2. Select multiple users entries by holding down control while selecting and/or deselecting.
3. Select multiple by holding down the shift button while selecting the first and then last of a collection.



*Figure 14 Available and Assigned Groups lists*

**Step 3:** Save the association by clicking **Update Association**.  No association is saved until this button is selected.

**Assign or Deassign Users and ProtectionElements:**

**Step 1:** Navigate to the Association screen.  From the element home page, either create a new element (see *Create New*) or search for and select an existing element (see *Search for and Select Existing Elements*).  The element's Details screen displays a button containing the text **Associated**, **Assign**, or something similar depending on the element type.

**Step 2:** With this UI implementation, associations can be established by selecting 'Assign'. The box lists the Assigned ProtectionElements.  Simply select **Deassign** to deassign and remove a PE from the Assigned PEs box.

There are multiple ways to highlight the elements within the box:

1. Select one by clicking on the user name entry.
2. Select multiple users entries by holding down control while selecting and/or deselecting.
3. Select multiple by holding down the shift button while selecting the first and then last of a collection.
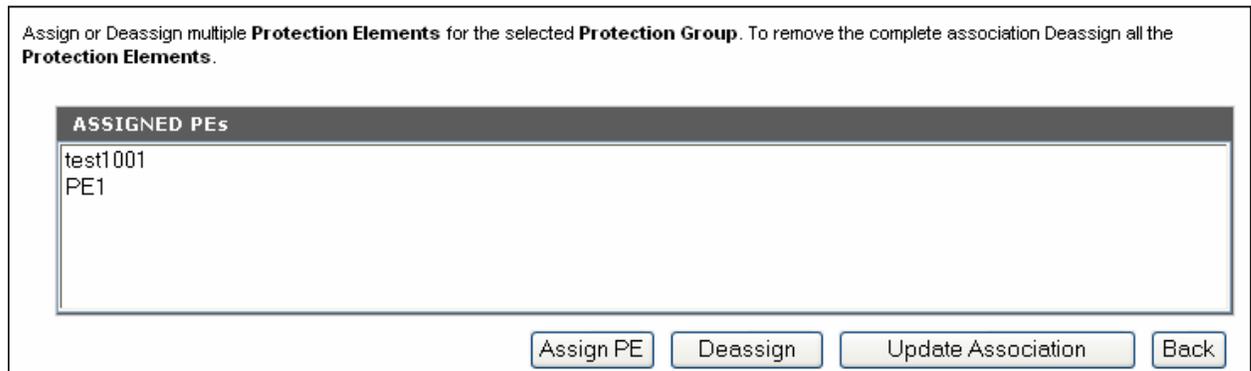


*Figure 15 Assigned PEs list*

On selecting the 'Assign PE' button, the popup search criteria screen is displayed.
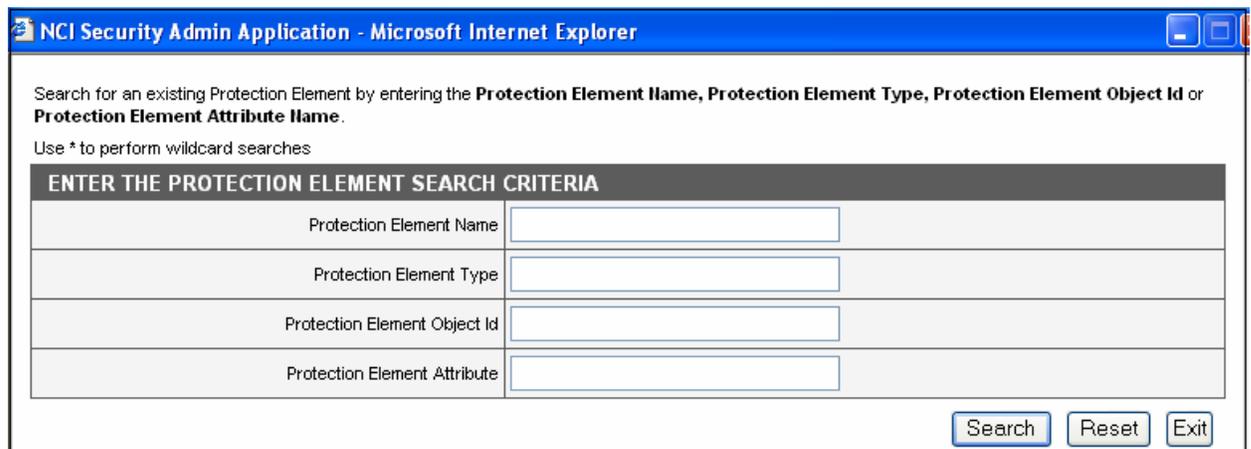


*Figure 16Protection Element search criteria popup screen.*

On clicking the search button the sorted search results for the given search criteria is displayed. One or more checkboxes can be selected for assignment by checking and clicking the 'Assign PE'. The selected PE's will be added to the Assigned PE's box.

.



*Figure 16 Protection Element search result popup screen.*



*Figure 17 Assigned PEs list.*

**Step 3:** Save the association by clicking **Update Association**.  No association is saved until this button is selected.

## Super Admin Mode

### Overview

The Super Admin Mode includes operations pertaining to Users (Application Administrators), Applications, and Privileges.  Super Admins. may add, remove, or modify Application details. They may also assign users to these Applications, modify user details, and remove users.  Lastly, they may modify existing CSM Standard Privileges or create new application-specific privileges.

## Workflow

The CSM team designed the UPT as a flexible tool with a flexible workflow. Any operation can be completed quickly, however, at first it may be difficult to know where to start. The following is a suggested workflow for getting started in the Super Admin Mode:

1. **Application** – when first deploying the UPT for a particular application, the developer registers the application in the *Application* section. (See the CSM Guide for Application Developers for details.)
2. **Application** – add and update Application details.
3. **User** – add and update users who will serve as Application Administrators.
4. **Application** – assign users to applications.
5. **Privilege** – if necessary, add or edit CSM Standard Privileges.

## Navigation

Use the gray menu to navigate through the Super Admin section. From the Home page, the menu looks like this:



*Figure 17 Home Page menu options*

The menu option with a blue background designates the current location. Roll over the other choices until they turn blue, and then click to navigate to that section. The **Log Out** selection returns the user to the Login page.

## Application

In the Application section, a Super Admin can add an application to the UPT and add or modify details. Here are the available operations to perform:

### 1. Create a New Application

    a. Go the Application home page.
    b. Select **Create a New Application**.
    c. Enter data into the Application Details form.
        1. **Application Name** – uniquely identifies the Application, required field.
        2. **Application Description** – a brief summary describing the Application.
        3. **Declarative Flag** – indicates whether application uses Declarative security.
        4. **Application Active Flag** – indicates if the Application is currently active.
        5. **Database URL** – The JDBC Database URL for the given application.
        6. **Database User Name** – The Username for the application database.

7. **Database Password** – The Password for the application database
8. **Database Dialect** – The Dialect for the application database.
9. **Database Driver** –The Driver for the application database

   Please note: the Database fields should either be completed together or left blank completely. They are all required fields if at least one of them is populated.

   d.  Select **Add** button.

## 2. Select an Existing Application and Update
   a.  Go to the Application home page.
   b.  Click on **Select an Existing Application**.
   c.  Enter data into the Application Search Criteria form.
       1. **Application Name** – uniquely identifies the Application.
   d.  Click on the radio button corresponding with the intended Application name.
   e.  Select **View Details**.
   f.  Enter data into the Application Details form.
       1. **Application Name** – uniquely identifies the Application, required field.
       2. **Application Description** – a brief summary describing the Application.
       3. **Declarative Flag** – indicates whether application uses Declarative security.
       4. **Application Active Flag** – indicates if the Application is currently active.
       5. **Database URL** – The JDBC Database URL for the given application.
       6. **Database User Name** – The Username for the application database.
       7. **Database Password** – The Password for the application database
       8. **Database Dialect** – The Dialect for the application database.
       9. **Database Driver** –The Driver for the application database

   Please note: the Database fields should either be completed together or left blank completely. They are all required fields if at least one of them is populated.

   g.  Select **Update** button.

## 3. Delete an Existing Application
   a.  Reach the Application Details form by either creating a new **Application** or **Selecting an Existing Application**.
   b.  Select **Delete**.
   c.  In the pop-up window, click **Okay** to confirm intent to delete.

## 4. Application and Admin Association
   a.  Reach the Application Details form by either creating a new Application or Selecting an Existing Application.
   b.  Select **Associated Admins**.

Ekagra

High Impact – High Value – Business Results

       1.     Associate Users (See *Assignments and Associations* for details).

   c. Click on the **Assign** and **Deassign** buttons until the proper association is displayed.

   d. Save the association by clicking on **Update Association**. No association is saved until this button is selected.

## User

In this section Users can be assigned as UPT administrators for their particular application(s). They will have the right to create and modify Roles, Groups, etc. In this section you may create new Users or modify exiting User details. Here are the available operations:

### 1. Create a New User

   a. Go to the User home page.

   b. Select **Create a New User.**

   c. Enter data into the User Details form.

- **Name** – uniquely identifies the User, required field.
- **First Name** and **Last Name** – attributes that help identify the User.
- **Organization** – Organization for which the User works. An example is the National Cancer Institute (NCI).
- **Department** – Department for which the User works. An example is caArray.
- **Title** – Title for User.
- **Phone Number** – provides contact information, typically the direct business phone number for the User. The phone number field accepts the following formats: 0123456789, 012-345-6789, (012)3456789, (012)345-6789, (012)-345-6789
- **Email Id** – provides the email contact details for the User. An email ID must contain an asterisk.
- **Password**– an optional field used if the schema for Authorization will also be used for Authentication. The only characters visible within this field are stars '*' so the password is not visible on the screen.
- **Confirm Password** – a copy of the password field. It ensures the intended password was entered correctly. This field must match the password field exactly.
- **User Start Date** and **User End Date** – determine the period for which the User is a valid User.

   d. Select **Add** button.

### 2. Select an Existing User and Update

   a. Go to the User home page.

   b. Click **Select an Existing User**.

   c. Enter data into the User Search Criteria form.

- **User Name** – uniquely identifies the User.

d.  Click on the radio button corresponding with the intended User name.
e.  Select **View Details**.
f.  Enter data into the User Details form.
    - **Name** – uniquely identifies the User, required field.
    - **First Name** and **Last Name** – attributes that help identify the User.
    - **Organization** – Organization for which the User works.  An example is the National Cancer Institute (NCI).
    - **Department** – Department for which the User works.  An example is caArray.
    - **Title** – Title for User.
    - **Phone Number** – provides contact information, typically the direct business phone number for the User.  The phone number field accepts the following formats: 0123456789, 012-345-6789, (012)3456789, (012)345-6789, (012)-345-6789
    - **Email Id** – provides the email contact details for the User.  An email ID must contain an asterisk.
    - **Password**– an optional field used if the schema for Authorization will also be used for Authentication.  The only characters visible within this field are stars '*' so the password is not visible on the screen.
    - **Confirm Password** – a copy of the password field.  It ensures the intended password was entered correctly.  This field must match the password field exactly.
    - **User Start Date** and **User End Date** – determine the period for which the User is a valid User.
g.  Select **Update** button.

## 3.  Delete an Existing User
a.  Reach the User Details form by either creating a new User or Selecting an Existing User.
b.  Select **Delete**.
c.  In the pop-up window, click **Okay** to confirm intent to delete.

## **Privilege**

A Privilege refers to any operation performed upon data. Assigning Privileges helps control access to important components of an application (Protection Elements).

The UPT installs with CSM Standard Privileges that were agreed upon by the Security Working Group.  These privileges include the following:

### *Standard Privileges*

Within CSM, users may possess one or more of the following privileges for a particular protection element:

| *Privilege Name* | *Privilege Definition* | *Applying the Privilege (Example)* |
|---|---|---|
| CREATE | This privilege grants permission to a user to create an entity.  This entity can be an object, a database entry, or a resource such as a network connection. | A user can create a database entry. |
| ACCESS | This privilege allows a user to access a particular resource.  Examples of resources include a network connection, database connection, socket, module of the application, or even the application itself. | A user can gain access to a particular module in an application. |
| READ | This privilege permits the user to read data from a file, URL, socket, database, or an object. This can be used at an entity level signifying that the user is allowed to read data about a particular entry (which can be object or database row, etc.) | A user can view personal information such as a Social Security Number. |
| WRITE | This privilege allows a user to write data to a file, URL, socket, database, or object. This can also be used at an entity level signifying that the user is allowed to write data about a particular entity (which may include an object, database row, etc.) | A user can add text to a database entry. |
| UPDATE | This privilege grants permission at an entity level and signifies that the user is allowed to update and modify data for a particular entity.  Entities may include an object, an attribute of the object, a database row, etc. | A user can modify an object's attribute data. |
| DELETE | This privilege permits a user to delete a logical entity. This entity can be an object, a database entry, a resource such as a network connection, etc. | A user can delete record. |

| EXECUTE | This privilege allows a user to execute a particular resource. The resource can be a method, function, behavior of the application, URL, button etc. | A user can click on a button to perform a method. |
|---------|-----|-----|

If necessary in this section you may create new application-specific Privileges or modify existing Privilege details.  Here are the available operations:

## 1. Create a New Privilege
   a.  Go to the Privilege home page.
   b.  Select **Create a New Privilege**.
   c.  Enter data into the Privilege Details form.
      - **Name** – uniquely identifies the Privilege, required field.
      - **Description** – a brief summary describing the Privilege.
   d.  Select **Add** button.

## 2. Select an Existing Privilege and Update details
   a.  Go to the Privilege home page.
   b.  Click **Select an Existing Privilege**.
   c.  Enter data into the Privilege Search Criteria form.  Search **Privilege** name.
   d.  Click on the radio button corresponding with the intended **Privilege** name.
   e.  Select **View Details**.
   f.  Enter data into the Privilege Details form.
      - **Name** – uniquely identifies the Privilege, required field.
      - **Description** – a brief summary describing the Privilege.
   g.  Select **Update** button.

## 3. Delete an Existing Privilege
   a.  Reach the Privilege Details form by either creating a new Privilege or Selecting an Existing Privilege.
   b.  Select **Delete**.
   c.  In the pop-up window, click **Okay** to confirm intent to delete.

## Admin Mode

### Overview

The Admin Mode of the UPT is divided into six major sections: *Groups*, *Privileges*, *Protection Groups*, *Roles*, and *Users*.  In these sections an Admin can perform basic functions such as modify, delete, or create, and manage associations between the objects. For example, you may assign Privileges to a Role.  Figure 18 helps to illustrate how all objects (also referred to as elements) are related in the Authorization schema. Table 1 follows with definitions of each category of authorization.
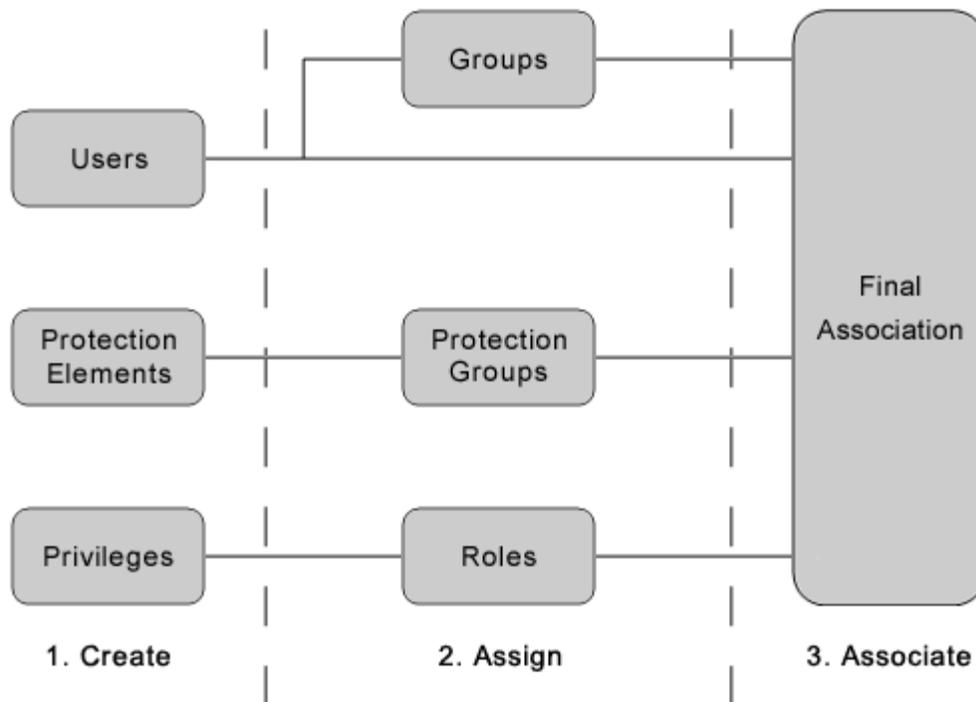


*Figure 18 Relationships between objects in the Authorization Schema*

| Definitions for Authorization Status | |
|---|---|
| User | A User is someone who requires access to your application. Users can become part of a Group, and can have an associated Protection Group and Roles. |
| Protection Element | A Protection Element is any entity (typically data) that has controlled access. Examples include **Social Security Numbe**r, **City**, and **Salary**. |
| Privilege | A Privilege refers to any operation performed upon data.  CSM makes use of a standard set of privileges.  This will help standardize authorization to comply with JAAS and Authorization Policy and allow for adoption of technology such as SAML in the future. |

| *Definitions for Authorization Status* | |
|---|---|
| Group | A Group is a collection of application users. By combining users into a Group, it becomes easier to manage their collective roles and access rights in your application. |
| Protection Group | A Protection Group is a collection of application Protection Elements. By combining Protection Elements into a Protection Group, it becomes easier to associate Users and Groups with rights to a particular data set. Examples include Address and Personal Information. |
| Role | A Role is a collection of application Privileges. Examples include Record Admin and EmployeeModify. |
| Final Association | The final association is the correlation between a User and his Roles for a particular Protection Group. |
| Each User (and Group) assumes Roles (rights) for a Protection Group (protected entities).  For example, User John has a Role EmployeeModify for all elements in the Address Protection Group. Assign PGs and Roles from the User or Group sections of the UPT. | |

*Table 1 Categories of authorization status*

### Workflow

The CSM team designed the UPT as a flexible tool with a flexible workflow.  Any operation can be completed quickly, however, at first it may be difficult to know where to start. The general concept of the workflow is to create the base elements first and then create the groupings and associations.  Here is the suggested workflow for getting started in the Admin Mode:

1. Create base objects – Users and Protection Elements (CSM Standard Privileges are provided).
2. Create collections of these objects (in any order):
    a. Groups
        i. Create Groups.
        ii. Assign Users to Groups.
    b. Protection Groups
        i. Create Protection Groups.
        ii. Assign Protection Elements to Protection Groups.
    c. Roles
        i. Create Roles.
        ii. Assign Privileges to Roles.
3. Associate rights with Users and Groups (in any order).
        i. Assign a Protection Group and Roles to Users.
        ii. Assign a Protection Group and Roles to Groups.

**Ekagra**

High Impact – High Value – Business Results

### Navigation

Use the gray menu to navigate through the Admin section.  From the Home page, the menu looks like this:

| HOME | USER | PROTECTION ELEMENT | PRIVILEGE | GROUP | PROTECTION GROUP | ROLE | LOG OUT |
|---|---|---|---|---|---|---|---|

*Figure 19 Menu options in the Admin section of the home page*

The menu option with a blue background designates the current location.  Roll over the other choices until they turn blue, and then click to navigate to that section.  The **Log Out** selection returns the user to the Login page.

### User

A User is simply someone that requires access to an application. In this section create new Users, modify existing User details, and associate or disassociate Users with a Protection Group and Roles.   The available operations are:

**1.  Create a New User**
   a.  Go to the User home page.
   b.  Select Create a New User.
   c.  Enter data into the User Details form.
   - **Name** – uniquely identifies the User, required field.
   - **First Name** and **Last Name** – attributes that help identify the User.
   - **Organization** – Organization for which the User works.  An example is the National Cancer Institute (NCI).
   - **Department** – Department for which the User works.  An example is caArray.
   - **Title** – Title for User.
   - **Phone Number** – provides contact information, typically the direct business phone number for the User.  The phone number field accepts the following formats: 0123456789, 012-345-6789, (012)3456789, (012)345-6789, (012)-345-6789
   - **Email Id** – provides the email contact details for the User.  An email ID must contain an asterisk.
   - **Password**– an optional field used if the schema for Authorization will also be used for Authentication.  The only characters visible within this field are stars '*' so the password is not visible on the screen.
   - **Confirm Password** – a copy of the password field.  It ensures the intended password was entered correctly.  This field must match the password field exactly.
   - **User Start Date** and **User End Date** – determine the period for which the User is a valid User.
   d.  Select **Add** button.

**2.  Select an Existing User and Update details**
   a.  Go to the User home page.

b. Click on **Select an Existing User**.
c. Enter data into the User Search Criteria form.  Search by any combination of the below:
   - **Name** – uniquely identifies the User, required field.
   - **First Name** and **Last Name** – attributes that help identify the User.
   - **Organization** – Organization for which the User works.  An example is the National Cancer Institute (NCI).
   - **Department** – Department for which the User works.  An example is caArray.
   - **Email Id** – provides the email contact details for the User.  An email ID must contain an asterisk.
d. Click on the radio button corresponding with the intended **User name**.
e. Select **View Details**.
f. Enter data into the User Details form.
   - **Name** – uniquely identifies the User, required field.
   - **First Name** and **Last Name** – attributes that help identify the User.
   - **Organization** – Organization for which the User works.  An example is the National Cancer Institute (NCI).
   - **Department** – Department for which the User works.  An example is caArray.
   - **Title** – Title for User.
   - **Phone Number** – provides contact information, typically the direct business phone number for the User.  The phone number field accepts the following formats: 0123456789, 012-345-6789, (012)3456789, (012)345-6789, (012)-345-6789
   - **Email Id** – provides the email contact details for the User.  An email ID must contain an asterisk.
   - **Password**– an optional field used if the schema for Authorization will also be used for Authentication.  The only characters visible within this field are stars '*' so the password is not visible on the screen.
   - **Confirm Password** – a copy of the password field.  It ensures the intended password was entered correctly.  This field must match the password field exactly.
   - **User Start Date** and **User End Date** – determine the period for which the User is a valid User.
g. Select **Update** button.

The User Details page displays the three buttons displayed in figure 18 below. The numbers above these buttons correspond to the operations that follow:



*Figure 20 User Details Page button options*

### 3. Assign a User to a Group or Groups ❸

a. Reach the User Details form by either creating a new User or Selecting an Existing User.
b. Select **Associated Groups**.
c. Determine which of the available Groups to which the User should be assigned. Select these Groups by highlighting them (See Assignments and Associations for details).
d. Click on the **Assign** and **Deassign** buttons until the proper association is displayed.
e. Save the association by clicking on **Update Association**.  **NOTE:** *No association is saved* until this button is selected.

### 4. View User Report ❹

This feature is new to the 3.0.1 release in response to a requirement formed by the caCORE team.  This reporting functionality shows a user's privileges for all of his protection elements.

a. Reach the User Details form by either creating a new User or Selecting an Existing User.
b. Select **Associated PE & Privileges.**
c. View user's privileges for each protection element.

### 5. Update Roles associated with the assigned Protection Groups ❺

a. Reach the User Details form by either creating a new User or Selecting an Existing User.
b. Select **Associated PG & Roles.**  The system displays a list of all associated Protection Groups and their Roles.
c. Select the radio button that corresponds with the intended Protection Group.
d. Determine which Roles you would like to assign to the User.
e. Select the Role by highlighting the name (See Assignments and Associations for details).
f. Click on the **Assign** and **Deassign** buttons until the proper association is displayed.
g. Save the association by clicking on **Update Association**.  **NOTE:** *No association is saved* until this button is selected.

### 6. Assign a Protection Group and Roles to a User ❻

a. Reach the User Details form by either creating a new User or Selecting an Existing User.
b. Select **Assign PG & Roles**.
c. Determine which Protection Group and Roles you would like to assign to the User.
   1. Select the Protection Group by highlighting the name (See Assignments and Associations for details).
   2. Select the Roles by highlighting them.

d. Click on the **Assign** and **Deassign** buttons until the proper association is
displayed.

e. Save the association by clicking on **Update Association**.  **NOTE:** *No association
is saved* until this button is selected.

### 7. Delete an Existing User
a. Reach the User Details form by either creating a new User or Selecting an Existing User.
b. Select **Delete**.
c. In the pop-up window, click **Okay** to confirm intent to delete.

## Protection Element

A Protection Element is any entity (typically data) that is subject to controlled access. CSM allows for a broad definition of Protection Element.  Nearly everything in an application can be protected – data, table, buttons, menu items, etc.  By identifying individual Protection Elements, it becomes easier to control access to important data.  In this section you may create new Protection Elements or modify existing Protection Element details.  Here are the available operations:

### 1. Create a New Protection Element
a. Go to the Protection Element home page.
b. Select **Create a New Protection Element**.
c. Enter data into the Protection Element Details form.
- **Name** – uniquely identifies the Protection Element, required field.
- **Object Id** – a string that the Application team assigns to the Protection Element
- **Attribute Name** – helps to further identify the Protection Element
- **Description** – a brief summary describing the Protection Element.
- **Update Date** – indicates the date when the Protection Element's Details were last updated
- **Type** – a string that the application team can assign to indicate type of protection element.
d. Select **Add** button.

### 2. Select an Existing Protection Element and Update details
a. Go to the Protection Element home page.
b. Click **Select an Existing Protection Element**.
c. Enter data into the Protection Element Search Criteria form.  Search by any combination of the fields below:
- **Name** – uniquely identifies the Protection Element.
- **Object Id** – a string that the Application team assigns to the Protection Element
- **Attribute Name** – helps to further identify the Protection Element
d. Click the radio button corresponding with the intended Protection Element name.
e. Select **View Details.**
f. Enter data into the Protection Element Details form.
- **Name** – uniquely identifies the Protection Element.
- **Object Id** – a string that the Application team assigns to the Protection Element

- **Attribute Name** – helps to further identify the Protection Element
- **Type** – a string that the application team can assign to indicate type of protection element.

g. Select **Update** button.

### 3. Delete an Existing Protection Element

a. Reach the Protection Element Details form by either creating a new Protection Element or Selecting an Existing Protection Element.
b. Select **Delete**.
c. In the pop-up window, click **Okay** to confirm intent to delete.

### 4. Assign a Protection Element to a Protection Group or Protection Groups

a. Reach the Protection Element Details form by either creating a new Protection Element or Selecting an Existing Protection Element.
b. Select **Associated PGs.**
c. Determine which of the available Protection Groups to which the Protection Element should be assigned.
　　1. Select these Protection Groups by highlighting them (See *Assignments and Associations* for details).
d. Click on the **Assign** and **Deassign** buttons until the proper association is displayed.
e. Save the association by clicking on **Update Association**. **NOTE: No association is saved** until this button is selected.

## Privilege

A Privilege refers to any operation performed upon data. Assigning privileges helps control access to important components of an application (Protection Elements). CSM provides a standard set of privileges that populate automatically when creating the authorization schema (See *Standard Privileges*).

Because Standard Privileges are provided the Privilege section does not contain Create, Delete, or Update functions. However, you may search for and view existing privileges. Use the Role section to assign privileges to roles.

### 1. Select an Existing Privilege

a. Go to the Privilege home page.
b. Click **Select an Existing Privilege**.
c. Enter data into the Privilege Search Criteria form. Search **Privilege** name.
d. Click on the radio button corresponding with the intended **Privilege** name.
e. Select **View Details**.
f. View data in the Privilege Details form.

- **Name** – uniquely identifies the Privilege, required field.
- **Description** – a brief summary describing the Privilege.

### Protection Group

A Protection Group is a collection of application Protection Elements.  By combining Protection Elements into a Protection Group, it becomes easier to associate Users and Groups with rights to a particular data set.  In this section you may create new Protection Groups, modify existing Protection Group details, assign Protection Elements, and assign a parent for a Protection Group.

The Protection Group is the only element that can have a Parent.  Using Parents is a way to group Protection Groups within Protection Groups.  This makes organizing users and their authorization rights easier.

Here are the available Protection Group operations:

1. **Create a New Protection Group**
   a. Go to the Protection Group home page.
   b. Select **Create a New Protection Group**.
   c. Enter data into the Protection Group Details form.
      - **Name** – uniquely identifies the Protection Group, required field.
      - **Description** – a brief summary describing the Protection Group.
      - **Large Count Flag** – used to indicate if the Protection Group has a large number of associated Protection Elements.
      - **Update Date** – indicates the date when this Protection Group's Details were last updated
   d. Select **Add** button.

2. **Select an Existing Protection Group and Update details**
   a. Go to the Protection Group home page.
   b. Click **Select an Existing Protection Group**.
   c. Enter data into the Protection Group Search Criteria form.  Search by **Protection Group** name.
   d. Click on the radio button corresponding with the intended **Protection Group** name.
   e. Select **View Details**.
   f. Enter data into the Protection Group Details form.
      - **Name** – uniquely identifies the Protection Group, required field.
      - **Description** – a brief summary describing the Protection Group.
      - **Large Count Flag** – used to indicate if the Protection Group has a large number of associated Protection Elements.
      - **Update Date** – indicates the date when this Protection Group's Details were last updated
   g. Select **Update** button.

3. **Delete an Existing Protection Group**
   a. Reach the Protection Group Details form by either creating a new Protection Group or Selecting an Existing Protection Group.
   b. Select **Delete**.

c.   In the pop-up window, click **Okay** to confirm intent to delete.

### 4. Assign Protection Elements to the Protection Group

a.   Reach the Protection Group Details form by either creating a new Protection Group or Selecting an Existing Protection Group.

b.   Select **Associated PEs**.

c.   Determine which of the available Protection Elements should be assigned to the Protection Group.

1.   Select these **Protection Groups** by highlighting them (See Assignments and Associations for details).

d.   Click on the **Assign** and **Deassign** buttons until the proper association is displayed.

e.   Save the association by clicking on **Update Association**. **NOTE:** *No association is saved* until this button is selected.

### 5. Assign a Parent for the Protection Group

a.   Reach the Protection Group Details form by either creating a new Protection Group or Selecting an Existing Protection Group.

b.   Select **Associated Parent PG**.

c.   Determine which available Protection Group should be designated as the Protection Group Parent.

1.   Select the **Parent** by highlighting the name.  Only one parent may be assigned.

d.   Click on the **Assign** and **Deassign** buttons until the proper association is displayed.

e.   Save the association by clicking on **Update Association**.  **NOTE:** *No association is saved* until this button is selected.

### Role

A Role is a collection of Privileges.  By combining Privileges into a Role, it becomes easier to associate Users and Groups with rights to a particular data set.  In this section you may create new Roles, modify existing Role details, and assign or deassign Privileges to the Role.  Here are the available operations:

### 1. Create a New Role

a.   Go to the Role home page.

b.   Select **Create a New Role**.

c.   Enter data into the Role Details form.

- **Name** – uniquely identifies the Role, required field.
- **Description** – a brief summary describing the Role.
- Active Flag – indicates if the Role is currently active.

d.   Select **Add** button.

## 2. Select an Existing Role and Update details

   a. Go to the Role home page.
   b. Click **Select an Existing Role**.
   c. Enter data into the Role Search Criteria form.  Search by Role name.
   d. Click the radio button corresponding with the intended Role name.
   e. Select **View Details**.
   f. Enter data into the Role Details form.
   - **Name** – uniquely identifies the Role, required field.
   - **Description** – a brief summary describing the Role.
   - **Active Flag** – indicates if the Role is currently active.
   g. Select **Update** button.

## 3. Delete an Existing Role

   a. Reach the Role Details form by either creating a new Role or Selecting an Existing Role.
   b. Select **Delete**.
   c. In the pop-up window, click **Okay** to confirm intent to delete.

## 4. Assign Privileges to the Role

   a. Reach the Role Details form by either creating a new Role or Selecting an Existing Role.
   b. Select **Associated Privileges**.
   c. Determine which of the available Privileges should be assigned to the Role.
      1. Select these **Roles** by highlighting them (See Assignments and Associations for details). Click on the **Assign** and **Deassign** buttons until the proper association is displayed.
   d. Save the association by clicking on **Update Association**.  **NOTE:** *No association is saved* until this button is selected.

## Group

A Group is a collection of application users. By combining users into a Group, it becomes easier to manage their collective roles and access rights in your application. Simply select an existing group, and associate a new Protection Group and Roles. Upon doing so, everyone in that particular Group has the same rights.

Under the User portion of UPT you may assign users to Groups. In this section you may create new Groups, modify existing Group details, and associate or disassociate Groups' Protection Groups and Roles. Here are the available operations:

## 1. Create a New Group

   a. Go to the Group home page.
   b. Select **Create a New Group**.
   c. Enter data into the Group Details form.
   - **Name** – uniquely identifies the Group, required field.
   - **Description** – a brief summary describing the Group.

    d.  Select **Add** button.

## 2. Select an Existing Group and Update details

    a.  Go to the Group home page.

    b.  Click on **Select an Existing Group**.

    c.  Enter data into the Group Search Criteria form.  Search by Group name.

    d.  Click on the radio button corresponding with the intended Group name.

    e.  Select **View Details**.

    f.  Enter data into the Group Details form.

        • **Name** – uniquely identifies the Group, required field.

        • **Description** – a brief summary describing the Group.

    g.  Select **Update** button.

The Group Details page displays the two buttons displayed in *Figure 21*. The numbers above these buttons correspond to the operations that follow:

❸ | ❹ | ❺ | ❻

| Associated Users | Associated PE & Privileges | Associated PG & Roles | Assign PG & Roles |

*Figure 21*

## 3. Associate Users ❸

    h.  Select Associated Users button.

    i.  The Group and User Association screen displays a list of Assigned Administrators.

    j.  Click Assign User to assign additional Users to the Group.

    k.  Click Deassign User to deassign users.

    l.  Select Update Association to save the changed associations.

    m.  Select Back to return to the Group details screen.

## 4. View Group Report ❹

This feature is new to the 3.0.1 release in response to a requirement formed by the caCORE team.  This reporting functionality shows a group's privileges for all of its protection elements.

    a.  Reach the Group Details form by either creating a new User or Selecting an Existing Group.

    b.  Select **Associated PE & Privileges**.

    c.  View group's privileges for each protection element.

## 5. Assign a Protection Group and Roles to a Group ❺

    d.  Reach the Group Details form by either creating a new Group or Selecting an Existing Group.

    e.  Select **Assign PG & Roles**.

    f.  Determine which Protection Group and Roles you would like to assign to the

NCICB

Group.
  1. Select the **Protection Group** by highlighting the name (See <u>Assignments and</u> <u>Associations</u> for details).
  2. Select the Roles by highlighting them.
g. Click on the **Assign** and **Deassign** buttons until the proper association is displayed.
h. Save the association by clicking on **Update Association**. **NOTE:** *No association is saved* until this button is selected.

## 6. Update Roles associated with the assigned Protection Groups ⑥

a. Reach the Group Details form by either creating a new Group or Selecting an Existing Group.
b. Select **Associated PG & Roles**.
c. The system displays a list of all associated Protection Groups and their Roles.
d. Select the radio button that corresponds with the intended Protection Group.
e. Determine which Roles you would like to assign to the Group.
  1. Select the **Role** by highlighting the name (See <u>Assignments and Associations</u> for details).
f. Click on the **Assign** and **Deassign** buttons until the proper association is displayed.
g. Save the association by clicking on **Update Association**. **NOTE:** *No association is saved* until this button is selected.

## 7. Delete an Existing Group

a. Reach the Group Details form by either creating a new Group or Selecting an Existing Group.
b. Select **Delete**.
c. In the pop-up window, click **Okay** to confirm intent to delete.