



Common Security Module (CSM)

User Provisioning Tool (UPT) User Guide

Version No: 1.1

Last Modified: 03/22/05

Author : Eric Copen, JJ Maurer
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 in CVS under security/docs.

Revision History

Version Number	Revision Date	Author	Summary of Changes
0.1	2/7/05	Eric Copen	Initial draft
0.2	2/9/05	Eric Copen	Complete draft
0.3	2/15/05	JJM	Review and editorials
1.0	2/16/05	Eric Copen	Final changes
1.1	3/22/05	Eric Copen, Jill Hadfield	Formatting, grammar, aesthetic changes, etc.

Review

Name	Team/Role	Version	Date Reviewed	Reviewer Comments
Vinay Kumar	Team Lead	0.2	2/14	Approved
JJ Maurer	Ekagra Management	0.2	2/15	Approved with minor changes
Jill Hadfield	Technical Writer	1.0	3/14 – 3/22	Approved with minor changes

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
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

Document Location	2
Related Documents	2
Introduction	4
Workflow	4
Super Admin.	4
Admin.	4
Login	5
Common Basic Functions	5
Create New	5
Search for and Select Existing Elements	6
Update	7
Delete	8
Assignments and Associations	9
Super Admin. Mode	10
Overview	10
Workflow	10
Navigation	10
Application	10
User	12
Admin. Mode	13
Overview	13
Workflow	15
Navigation	15
User	16
Protection Element	18
Privilege	20
Protection Group	20
Role	22
Group	23

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, Privileges, 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 on page 10.

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 on page 15*.

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. **Security** is used in Figure 2.

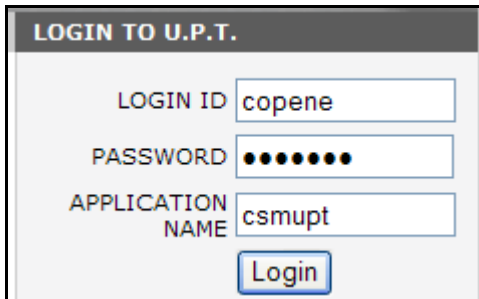


Figure 1 Login as a Super Admin.

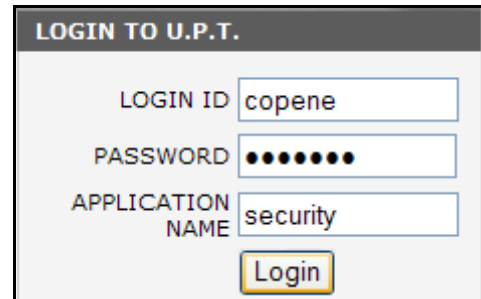


Figure 2 Login as an Admin.

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)

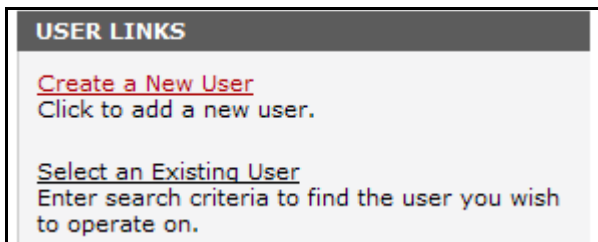


Figure 3 New and Existing User options

Step 2: Enter details (Figure 4):

* indicates a required field

ENTER THE NEW USER DETAILS	
* User Login Name	<input type="text" value="smithj"/>
User First Name	<input type="text" value="John"/>
User Last Name	<input type="text" value="Smith"/>
User Organization	<input type="text" value="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 (Figure 5).

<input type="button" value="Back"/>	<input type="button" value="Update"/>	<input type="button" value="Delete"/>	<input type="button" value="Associated Groups"/>	<input type="button" value="Associated PG & Roles"/>	<input type="button" value="Assign PG & Roles"/>
-------------------------------------	---------------------------------------	---------------------------------------	--------------------------------------------------	----------------------------------------------------------	------------------------------------------------------

Figure 5 A new set of buttons appear below the menu after you have successfully added a new user

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 could not insert: [gov.nih.nci.security.authorization.domainobjects.User]

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 Privilege is searched for and selected.

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

PRIVILEGE LINKS
Create a New Privilege Click to add a new privilege.
Select an Existing Privilege Enter search criteria to find the privilege you wish to operate on.

Figure 8 Selecting an existing privilege

Step 2: Enter search criteria. Use the * character to perform wildcard searches (see Figure 9). For example, searching for priv* returns privilege1, priv2, or any other privilege beginning with priv. A search of *1 returns anything ending with 1 – privilege1, priv1, read1, etc. **Select Search** for results. **Back** returns the user to the home page. **Reset** clears the data.

ENTER THE PRIVILEGE SEARCH CRITERIA	
Privilege Name	<input type="text" value="*1"/>
<div> <input type="button" value="Back"/> <input type="button" value="Search"/> <input type="button" value="Reset"/> </div>	

Figure 9 Entering search criteria for Privilege

Step 3: The system returns a list of matching privileges (Figure 10):

SEARCH RESULTS		
Select	Privilege Name	Privilege Description
<input type="radio"/>	Kunal1	Modi_tp
<input type="radio"/>	priv1	priv1 desc.
<input type="radio"/>	test_privilege1	privilege desc.

Figure 10 Privilege search results

Step 4: Select the desired element, in this case **priv1**, by clicking on the radio button in the **Select** column (Figure 11). You can select one element at a time to view.

<input checked="" type="radio"/>	priv1	priv1 desc.
----------------------------------	-------	-------------

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 4.1) or search for and select an existing element (See 4.2). The details screen 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 on page 6 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 on page 5) or search for and select an existing Group (see Search for and Select Existing Elements on page 6). 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, one may assign the **Privileges Create, Read, and Delete** to the Role General Administrator.

Step 1: Navigate to the Association screen. From the element home page, either create a new element (see Create New on page 5) or search for and select an existing element ((see Search for and Select Existing Elements on page 6). The element's Details screen displays a button containing the text **Associated, Assign**, or something similar depending on the element type.

Step 2: Assign or Deassign. 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 left lists the **Available Privileges** (unassigned) and the box on the right lists the **Privileges** assigned to the Role – **Create** and **Read**. Simply highlight a Privilege and select **Assign** to move it to the Assigned Privileges box. Select **Deassign** to move it back to the Available Privileges box.

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

1. Select one by clicking on the user name.
2. Select multiple users 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.

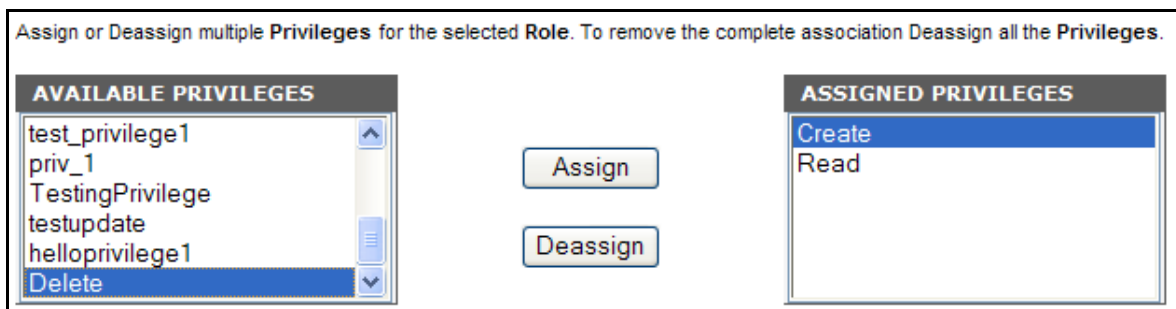


Figure 14 Available and Assigned Privilege lists

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) and Applications. Super Admins. may add, remove, or modify Application details. They may also assign users to these Applications, modify user details, and remove users.

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.

Navigation

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

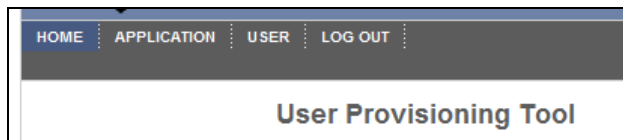


Figure 15 Home Page menu options

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.
- 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.
- 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.**
- c. Determine which of the available users should be assigned to the Application.
 1. Select these users by highlighting them (See [Assignments and Associations](#) on page 9 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**. 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 used for Authorization will also be used for Authentication.
 - **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 used for Authorization will also be used for Authentication.
 - **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.

Admin. Mode

Overview

The Admin. Mode of the UPT is divided into six major sections: *Groups*, *Privileges*, *Protection Groups*, *Roles*, and *Users*. These sections describe basic functions such as modify, delete, or create, and managing associations between the objects. For example, you may assign Privileges to a Role. Figure 16 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.

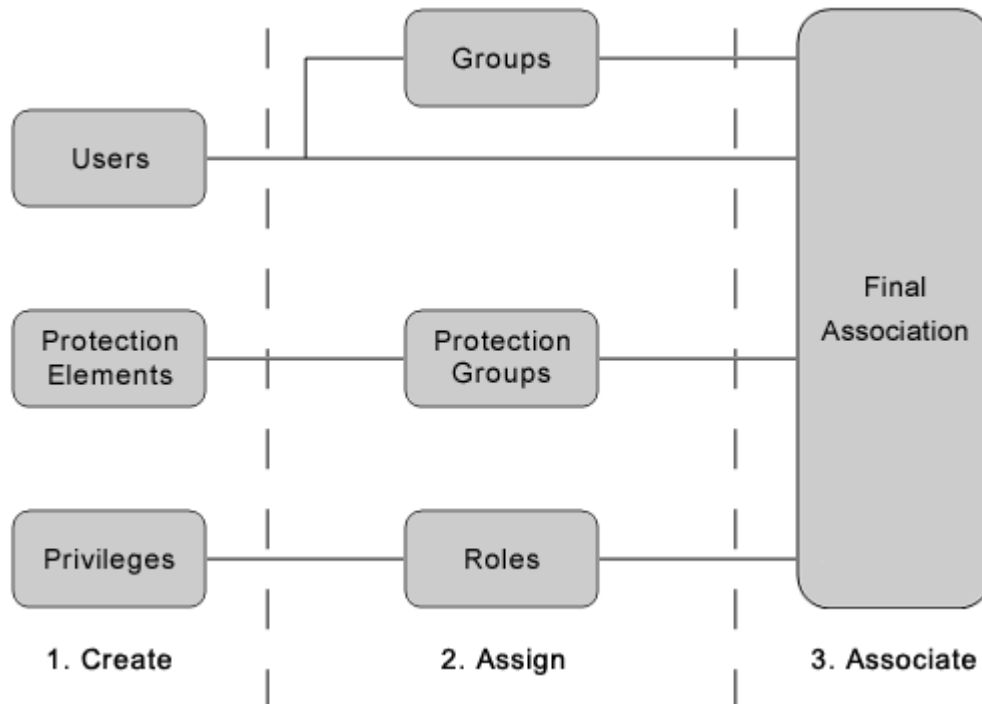


Figure 16 Relationships between objects in the Authorization Schema

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 Number , City , and Salary .
Privilege Privilege	A Privilege refers to any operation performed upon data. Examples include Delete Record or Modify Record .
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.

Definitions for Authorization Status	
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, Protection Elements, and Privileges (in any order).
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.

Navigation

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

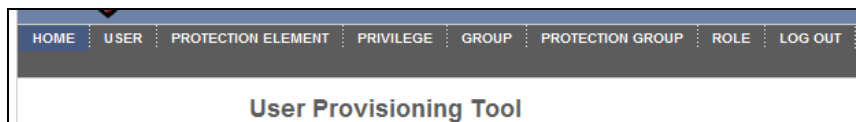


Figure 17 Menu options in the Admin section of the home page

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 used for Authorization will also be used for Authentication.
 - **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 used for Authorization will also be used for Authentication.
 - **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 6.4 below. The numbers above these buttons correspond to the operations that follow:

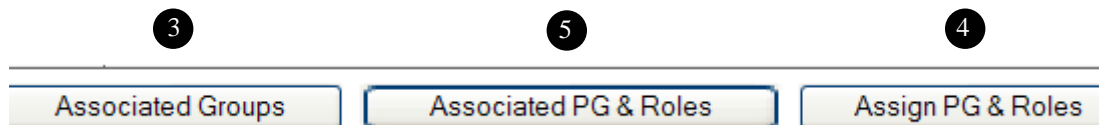


Figure 18 User Details Page button options

3. Assign a User to a Group or Groups ③

- 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](#) on page 9 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. Assign a Protection Group and Roles to a User ④

- 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](#) on page 9 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.

5. Update Roles associated with the assigned Protection Groups ⑤

- a. Reach the User Details form by either creating a new User or Selecting an Existing User.
- b. Select **Associated PG & Roles**.
- c. The system will display 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 User.
 1. Select the Role by highlighting the name (See [Assignments and Associations](#) on page 9 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. 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 Privilege's Details were last updated
- 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
- 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](#) on page 9 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. By identifying individual Privileges, it becomes easier to control access to important application data. In this section you may create new 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.

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](#) on page 9 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 PEs**.
- c. Determine which of the available Privileges should be assigned to the Role.
 1. Select these **Roles** by highlighting them (See [Assignments and Associations](#) on page 9 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 19*. The numbers above these buttons correspond to the operations that follow:



Figure 19

3. Assign a Protection Group and Roles to a Group

- a. Reach the Group Details form by either creating a new Group or Selecting an Existing Group.
- b. Select **Assign PG & Roles**.
- c. Determine which Protection Group and Roles you would like to assign to the Group.
 1. Select the **Protection Group** by highlighting the name (See [Assignments and Associations](#) on page 9 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.

4. Update Roles associated with the assigned Protection Groups

- 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 will display 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 [Assignments and Associations](#) on page 9 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.

5. 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.