

7 - Administering User Accounts

This chapter describes the process for creating and managing user accounts in calIntegrator. It also discusses the processes for managing ownership and access to studies in calIntegrator.

This chapter includes the following topics.

- [Overview of Administering calIntegrator User Accounts Using UPT](#)
- [Workflow for Creating User Access to calIntegrator](#)
 - [Creating a New calIntegrator User](#)
 - [Adding a User to a User Group](#)
 - [Creating a New User Group](#)
 - [Assigning a User Group to a Protection Group](#)
 - [Creating a New Protection Group](#)
 - [Changing a User Password](#)



Note

The options for performing user management tasks are visible in calIntegrator on the left sidebar of the browser only if you have these Admin privileges.

Overview of Administering calIntegrator User Accounts Using UPT



New User?

If you are interested in registering an account in calIntegrator, see [Registering as a New calIntegrator User](#).

In calIntegrator, all tasks related to creating and managing user accounts can be performed only by a calIntegrator administrator using the CBIIT User Provisioning Tool (UPT) v. 4.2. The following sections discuss the use of the UPT for performing these tasks. For further information about UPT, see Chapter 3 of the [CSM 5.0 Programmer's Guide](#).

The UPT is a separately installed application which serves as the user management interface for all National Cancer Institute CBIIT Life Sciences Distribution (LSD) applications, including calIntegrator. The UPT application is the central point for all user management functionality within calIntegrator. You can use UPT to add new users and to apply user group assignments to the calIntegrator database directly. The UPT groups can refer to predefined groups such as Study Manager or Study Investigator, which determine what roles the user has.

The following terms are used both in this chapter and in the UPT to define user-related roles:

- **User** – a person who is accessing calIntegrator. The user has an associated account and user ID.
- **User Group** – a group of users, typically grouped by organization and role, for example, "Columbia University Study Managers"
- **Protection Group** – a group of studies given a secure status and typically grouped by organization, for example, "Columbia University Protected Studies".

Workflow for Creating User Access to calIntegrator

The following steps summarize the process for establishing user access to calIntegrator:

1. A potential user requests a user account in calIntegrator. See [Registering as a New calIntegrator User](#).
2. You, as a calIntegrator administrator, check if the **User** already exists in calIntegrator. If not, [create the new User](#).
3. [Link the new User to a User Group](#). A "group" is a collection of users. Check if the requestor's **User Group** already exists in calIntegrator. If not, [create a new User Group](#).
4. [Link the User Group to a Protection Group](#). Check if the **Protection Group** (for example, "Columbia University Protected Studies"), containing the studies to which this new user wants access currently exists. If not, [create a new Protection Group](#).



Protection Group Access

If the Protection Group already exists, contact the Organizational Contact person to confirm that it is OK to give this person access to this Protection Group.

5. Give the requestor's **User Group** access to the **Protection Group**. See [Assigning a User Group to a Protection Group](#).

Creating a New calIntegrator User

To create a new **User** in calIntegrator, follow these steps:

1. Log into UPT as a calIntegrator Admin.
2. Search to see if the user already exists. Click the **User** menu option.
3. On the User page that opens, click **Select an Existing User**.

4. Use the form and search for the user. If you define no criteria, UPT returns a list of all calIntegrator users currently in the system. See the following figure for an example.

The screenshot shows the UPT interface with a navigation bar at the top containing links: HOME, USER, PROTECTION ELEMENT, PRIVILEGE, GROUP, PROTECTION GROUP, ROLE, INSTANCE LEVEL, and LOG OUT. The top right corner displays the user's login information: Login ID: boatt, Application: calIntegrator2, and Role: Admin. The main heading is "User". Below it is a "SEARCH RESULTS" table with the following columns: Select, User Login Name, User First Name, User Last Name, User Organization, User Department, and User Email Id. The table lists 13 users, including admin, cal2admin, gumanager, investigator, manager, manager2, manager3, manager4, manager5, nblamanager, and tcgaprivate. At the bottom right of the table are two buttons: "View Details" and "Back".

Select	User Login Name	User First Name	User Last Name	User Organization	User Department	User Email Id
☐	admin	UPT	Administrator			
☐	cal2admin	cal2	Admin			
☐	gumanager	Georgetown	Study Manager			
☐	investigator	Research	Investigator			
☐	manager	Study	Manager			
☐	manager2	Study	Manager2			
☐	manager3	Study	Manager3			
☐	manager4	Study	Manager4			
☐	manager5	Study	Manager5			
☐	nblamanager	NBLA	Study Manager			
☐	tcgaprivate	TCGA	Manager			

5. If the user does not already exist (is not listed in the search results), then create a new user. To do so, select the **User** menu option again, then click **Create a New User**. This opens the page for creating a new calIntegrator user.
6. Enter details only for the following required fields:
- **User Login Name**
 - **User First Name**
 - **User Last Name**
 - **User Password**



Caution

If the requestor is an LDAP user, then the User Login Name must match the LDAP login ID AND the User Password field must be left blank. If the requestor is not an LDAP user, then provide a password.

7. Click **Add** to confirm the new user.

At this point, you can add the new user to a [user group](#) where you can assign roles to the user, and the user group to a [protection group](#) where you can assign limited visibilities to the new user.



It is possible for administrators to use a 3rd-party tool to create calIntegrator users and passwords, then link this system to UPT. For more information about this option, contact [CBIIT Application Support](#).

Adding a User to a User Group

Once you have created a new user, that user can be linked to a collection of users called a [user group](#); the user group would then be assigned to a [protection group](#).

Assigning Users to Groups greatly improves the ease with which you, the admin, can provision access rights. You can instantly assign a role and protection group to an entire group of users instead of repeating the same assignment for each individual user.

For example, you can assign a new user to a user group to which you have already assigned a specific role, and then assign that user group to the protection group, or you can assign a role collectively to a protection group after it is created. If a user group and/or protection group with your selected role(s) does not exist, then you can [create such a group](#). For more information about roles, see [calIntegrator Roles](#).

To add a user to an existing user group, follow these steps:

1. Log into UPT as calIntegrator Admin.
2. Find the user that you want to assign to a user group. Click the **User** menu option, then click **Select an Existing User**.

- Enter the name of the user you are looking for and click **Search**. If you define no criteria, UPT returns a list of all calIntegrator users currently in the system, as shown in the following figure.

The screenshot shows the UPT interface. At the top, there is a header with the logo and text: "Common Security Module User Provisioning Tool". On the right, it displays "Login ID : boalt", "Application : calIntegrator2", and "Role : Admin". Below the header is a navigation bar with tabs: HOME, USER, PROTECTION ELEMENT, PRIVILEGE, GROUP, PROTECTION GROUP, ROLE, INSTANCE LEVEL, and LOG OUT. The main content area is titled "User". Below this is a "SEARCH RESULTS" table with the following columns: Select, User Login Name, User First Name, User Last Name, User Organization, User Department, and User Email Id. The table lists 12 users, including admin, cal2admin, gumanager, investigator, manager, manager2, manager3, manager4, manager5, nblmanager, and tcgaprivate. At the bottom right of the table are buttons for "View Details" and "Back".

Select	User Login Name	User First Name	User Last Name	User Organization	User Department	User Email Id
☐	admin	UPT	Administrator			
☐	cal2admin	cal2	Admin			
☐	gumanager	Georgetown	Study Manager			
☐	investigator	Research	Investigator			
☐	manager	Study	Manager			
☐	manager2	Study	Manager2			
☐	manager3	Study	Manager3			
☐	manager4	Study	Manager4			
☐	manager5	Study	Manager5			
☐	nblmanager	NBIA	Study Manager			
☐	tcgaprivate	TCGA	Manager			

- Select the radio button next to the name and click **View Details**. The User Details page open, showing brief details about the user you selected.
- Click the **Associated Groups** button at the bottom of the page. This opens the page where you can assign a user to a group, as shown in the following figure. The user you selected displays at the top of the page.

The screenshot shows the "User and Groups Association" page. At the top, it says "SELECTED USER" and displays "User Login Name: manager". Below this is a message: "Assign or Deassign multiple Groups for the selected User. To remove the complete association Deassign all the Groups." There are two main sections: "AVAILABLE GROUPS" and "ASSIGNED GROUPS". The "AVAILABLE GROUPS" section lists: Study Managers Group 3, Study Managers Group 4, Study Managers Group 5, NCI Study Investigators, and TCGA Study Managers. The "ASSIGNED GROUPS" section lists: Platform Manager Group and NCI Study Managers. Between these sections are buttons for "Assign" and "Deassign". At the bottom right are buttons for "Update Association" and "Back".

- In the Available Groups list, select one or more groups that you want the user to be in and click **Assign**. If such a group does not exist, you can [create a new user group](#).
- At the bottom of the page click **Update Association**. This completes the assigning of the user to the user group. Now the user will have access to any studies to which the user group has been given access.



User in Multiple Groups

You can add a user to more than one user group. For example, a user could be assigned to "Columbia University Study Managers" as well as to "Columbia University Study Investigators".

Creating a New User Group

To create a new user group in calIntegrator, follow these steps:

- Login to UPT as calIntegrator Admin.

2. If a user group that meets your specifications does not already exist, then you can create a new and unique user group. Click the **Group** menu option, then click **Create a new Group**.
3. On the form that opens, enter a unique **Group Name** and a description, if appropriate. Click **Add**.
4. Follow the directions in [Adding a User to a User Group](#) to link the new user to the new group you created.



Naming Convention

The recommended naming convention for a new User Group is *[insert organization name] Study [insert role]s*. Example: "Columbia University Study Managers".

Assigning a User Group to a Protection Group

To give a user group access to a protection group (a group of protected studies), follow these steps:

1. Login to UPT as calIntegrator Admin.
2. Find the user group you want to assign to the the protection group.
3. Click the **Group** menu option and click **Select an Existing Group**.
4. In the page that opens, click **Search**. If you define no criteria, UPT returns a list of all calIntegrator groups currently in the system. An example is shown in the following figure.

Group

SEARCH RESULTS		
Select	Group Name	Group Description
☐	Study Managers Group 3	Study Managers who can create/modify any Group 3 studies.
☐	Study Managers Group 4	Study Managers who can create/modify any Group 4 studies.
☐	Study Managers Group 5	Study Managers who can create/modify any Group 5 studies.
☐	NCI Study Investigators	Study investigators for the NCI studies.
☐	NCI Study Managers	Study Managers who can create/modify any NCI studies.
☐	Platform Manager Group	The platform manager group.
☐	TCGA Study Managers	Study Managers who can create/modify any TCGA studies.

[View Details](#)
[Back](#)

5. Select the radio button next to the group name you want to assign to the protection group, and click **View Details**. This opens the Group Details page. An example is shown in the following figure.

Common Security Module
User Provisioning Tool

Login ID : boelt
 Application : calIntegrator2
 Role : Admin

[HOME](#) | [USER](#) | [PROTECTION ELEMENT](#) | [PRIVILEGE](#) | [GROUP](#) | [PROTECTION GROUP](#) | [ROLE](#) | [INSTANCE LEVEL](#) | [LOG OUT](#)

Update the details of the displayed Group. The **Group Name** uniquely identifies the Group and is a required field. The **Group Description** is a brief summary about the Group. The **Update Date** indicates the date when this Group's Details were last updated.

GROUP DETAILS	
Group Name	NCI Study Managers
Group Description	Study Managers who can create/modify any NCI studies.
Group Update Date	09/24/2009 (MM/DD/YYYY)

[Update](#)
[Delete](#)
[Back](#)

[Associated Users](#)
[Associated PE & Privileges](#)
[Associated PG & Roles](#)
[Assign PG & Roles](#)

6. Below the group details, click **Associated PG & Roles**. The page that opens, shown in the following figure, displays any PG to which the user group is already assigned.

Group, Protection Group and Roles

SELECTED GROUP

	Group Name	NCI Study Managers
--	------------	--------------------

Select the **Protection Group** association which to be removed for the selected **Group** or whose **Roles** Association needs to be updated.

SEARCH RESULTS		
Select	Associated Protection Group Name	Associated Role Name
☐	NCI Protected Studies	STUDY_MANAGER_ROLE

[Remove PG & Roles](#)
[Associated Roles](#)
[Back](#)

- Below the group name, examine if the protection group of your choice is already listed there. If so, this means your user group is already assigned to the protection group of choice, and you can skip the remainder of the steps in this section. If the Protection Group is not listed there, then click **Back**.
- Back on the User Group details page, click **Assign PG & Roles**. This opens the Group, Protection Group and Rules Association page where you can assign a role to the user. calintegrator roles are defined in the following table:

Role Name	Role Definition
STUDY_MANAGER_ROLE	Assigning this role allows the user to modify existing studies, create new studies, and deploy existing studies.
STUDY_INVESTIGATOR_ROLE	Assigning this role allows the user to search the study, save queries about the study and perform analyses.
PLATFORM_MANAGER_ROLE	Assigning this role allows the user to create and delete array platforms for the entire calintegrator installation. Caution: Array platforms are shared by all users and studies in the calintegrator installation. A user with this role can affect the platforms that are used by all users and studies in the calintegrator installation.

- If this user group is a group of study managers, then select STUDY_MANAGER_ROLE. If this user group is a group of study investigators, then select STUDY_INVESTIGATOR_ROLE. After making your selection, click **Assign**.

Click **Update Association** at the bottom of the page. This completes the assigning of the user group to the protection group you chose.



Roles Across Groups

If a **User** has the STUDY_MANAGER_ROLE role for more than one **Protection Group**, then any study that the **User** creates will be assigned to each of those **Protection Groups**.

Creating a New Protection Group

If the Protection Group with the appropriate settings does not exist, you can create a new protection group by following these steps.

- Login to UPT as calintegrator Admin.
- Click the **Protection Group** menu option.
- On the page that opens, click **Create a New Protection Group**. The page opens for defining PG Group details, shown in the following figure.

Common Security Module
User Provisioning Tool

Login ID : boait
Application : calintegrator2
Role : Admin

HOME USER PROTECTION ELEMENT PRIVILEGE GROUP PROTECTION GROUP ROLE INSTANCE LEVEL LOG OUT

Enter the details to add a new Protection Group. The **Protection Group Name** uniquely identifies the Protection Group and is a required field. The **Protection Group Description** is a brief summary about the Protection Group. The **Protection Group Large Count Flag** is used to indicate if the Protection Group has a large number of associated Protection Elements.

* indicates a required field

ENTER THE NEW PROTECTION GROUP DETAILS

* **Protection Group Name**

Protection Group Description

Protection Group Large Count Flag ☐ Yes ☒ No

Add Reset Back

- Enter a unique **Protection Group Name** and **Description**, if appropriate. Click **Add**.



Naming Convention

The recommended naming convention is *[insert organization name here] Protected Studies*. Example: "Columbia University Protected Studies".

Changing a User Password

To change a password for a user, follow these steps:

- Confirm if the user is an LDAP user or not. If the user is an LDAP user, then this person must change their password using the NCI password change utility. Skip the rest of these steps. If the user is not an LDAP user, then continue with the rest of these steps.
- Log into UPT as calintegrator Admin.
- Find the user that you want to change. Click the **User** menu option, then **Select an Existing User**.
- Enter the name of the user you are looking for and click **Search**. If you define no criteria, UPT returns a list of all calintegrator users.
- Select the radio button next to the name and click **View Details**.

6. In the page that opens, shown in the following figure, replace the **User Password** and **Confirm Password** fields with the new password.

**Common Security Module
User Provisioning Tool**

Login ID : **boalt**
Application : **calIntegrator2**
Role : **Admin**

HOME | USER | PROTECTION ELEMENT | PRIVILEGE | GROUP | PROTECTION GROUP | ROLE | INSTANCE LEVEL | LOG OUT

Update the details of the displayed User. The **User Login Name** uniquely identifies the User and is a required field. The **User First Name** and **User Last Name** identifies the User. The **User Organization**, **User Department** and **User Title** provides his work details. The **User Phone Number** and **User Email Id** provides the contact details for the User. The **User Password** can be entered if the same schema is also going to be used for Authentication. The **User Start Date** and **User End Date** determine the period for which the User is a valid User. The **Update Date** indicates the date when this User's Details were last updated.

USER DETAILS	
* User Login Name	manager
* User First Name	Study
* User Last Name	Manager
User Organization	
User Department	
User Title	
User Phone Number	
User Password	••••••
Confirm Password	••••••
User Email Id	
User Start Date	(MM/DD/YYYY)
User End Date	(MM/DD/YYYY)
User Update Date	09/24/2009 (MM/DD/YYYY)

UpdateDeleteBack

Associated GroupsAssociated PE & PrivilegesAssociated PG & RolesAssign PG & Roles

7. At the bottom of the page click **Update**.