Bioinformatics Integration Support Contract (BISC)

IMMPORT ADMIN FUNCTIONAL REQUIREMENTS

Version 1.0

Period Of Performance: September 30, 2012 to September 29, 2017

Project Sponsor:

National Institutes of Health (NIH)
National Institute of Allergy and Infectious Diseases (NIAID)
Division of Allergy, Immunology, and Transplantation (DAIT)

Prepared by:

NORTHROP GRUMMAN

Northrop Grumman Corporation
Information Systems Sector
Health IT
2101 Gaither Road, Suite 600
Rockville, MD 20850
(301)527-6400 Main
(301)527-6401 Fax
Jeff.Wiser@ngc.com

Contents

IMMPORT ADMIN FUNCTIONAL REQUIREMENTS iii
Version 1.0 iii
Period Of Performance: September 30, 2012 to September 29, 2017 iii
Project Sponsor: iii
Prepared by: iii
1.1 User Management and Authentication 3
1.2 Program, Contract, Project Management 62
1.3 Menus Options 84

ImmPort Private Functional Requirements Version History

Version	Date	Description
1.0	3/31/2016	Initial version of the ImmPort 3.0 Administrative requirements

1.1 USER MANAGEMENT AND AUTHENTICATION

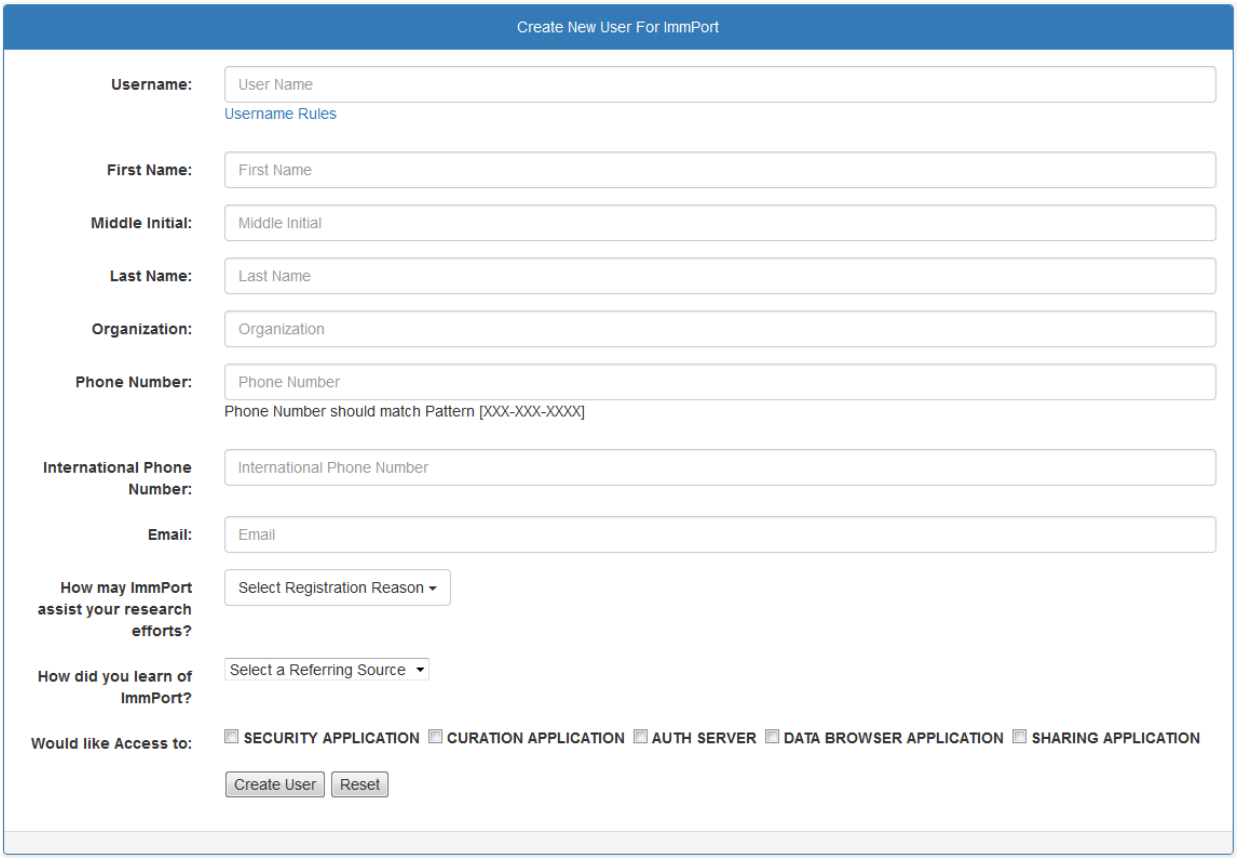
1.1.1 Description

The Manage User design artifacts model system administration capabilities, which include allowing users to request system access (register) creating user accounts, updating user information, querying users, and deactivating users from the system.

1.1.2 Detailed Design

1.1.2.1 Create/View/Update/Search User

The Create/View/Update/Search User depicts the events for creating/viewing/updating/searching a user account. The system collects the user information and creates a user account, provided the submitted data are valid. Once the user information is collected the system will display the data while giving the user an option to update the information.



1.1.2.2 Create New User Use Case

Actor: A user with the SECURITY_USER ROLE

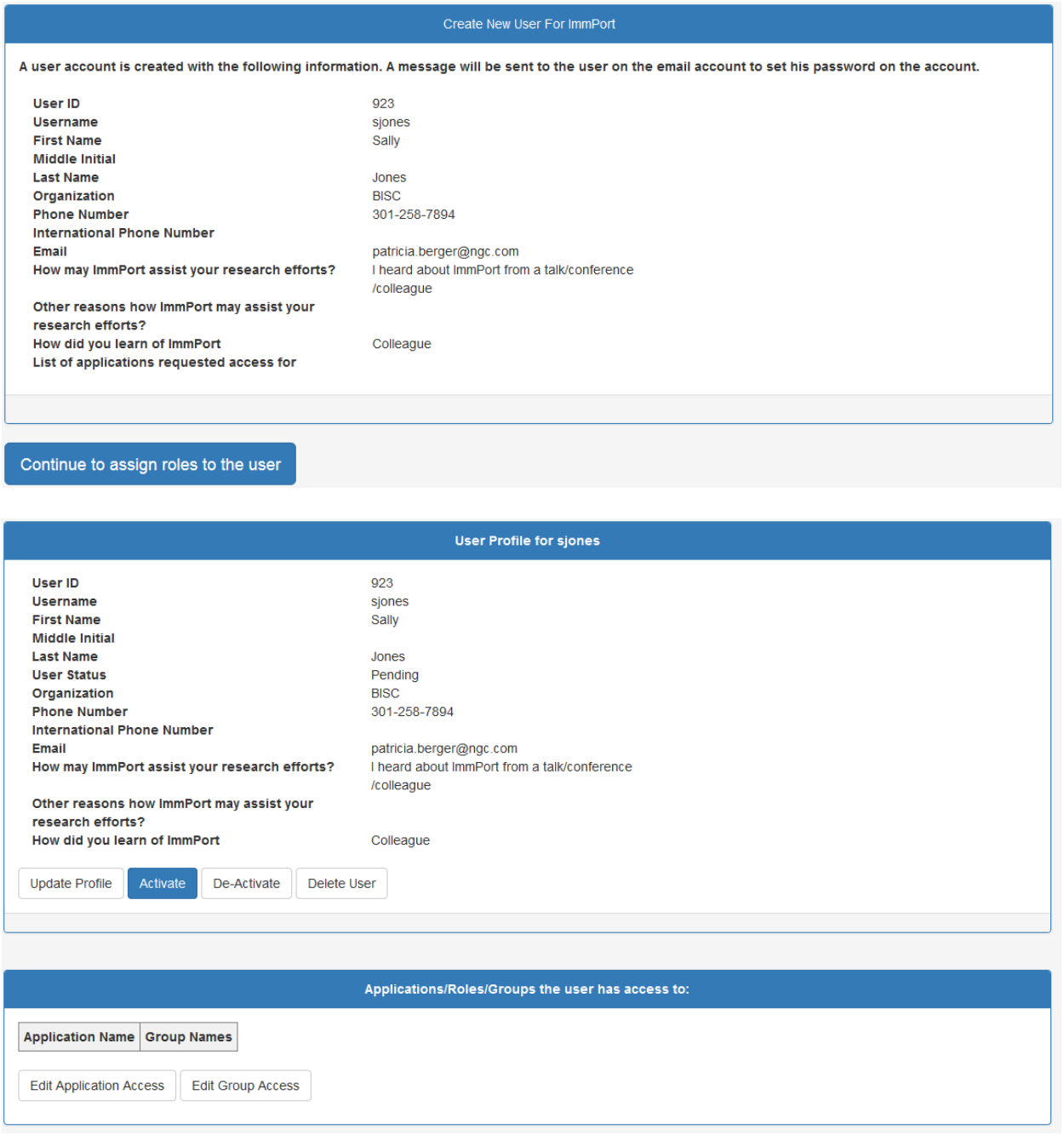
Pre-Conditions: The actor has access to the Security Application

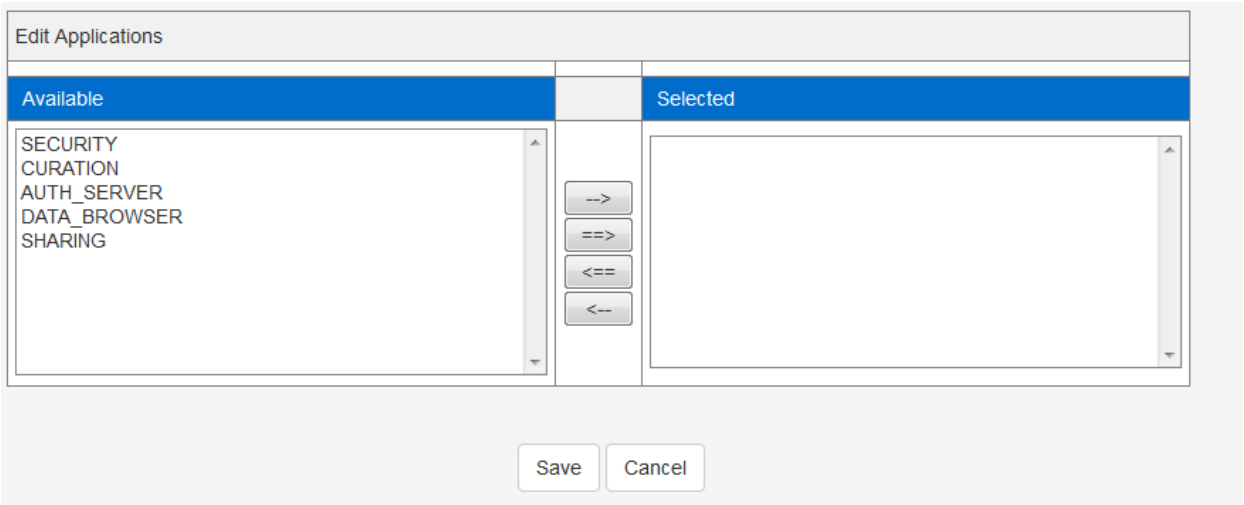
Post-Conditions: A user is created in the system with a default User Role and the default Roles of the Applications.

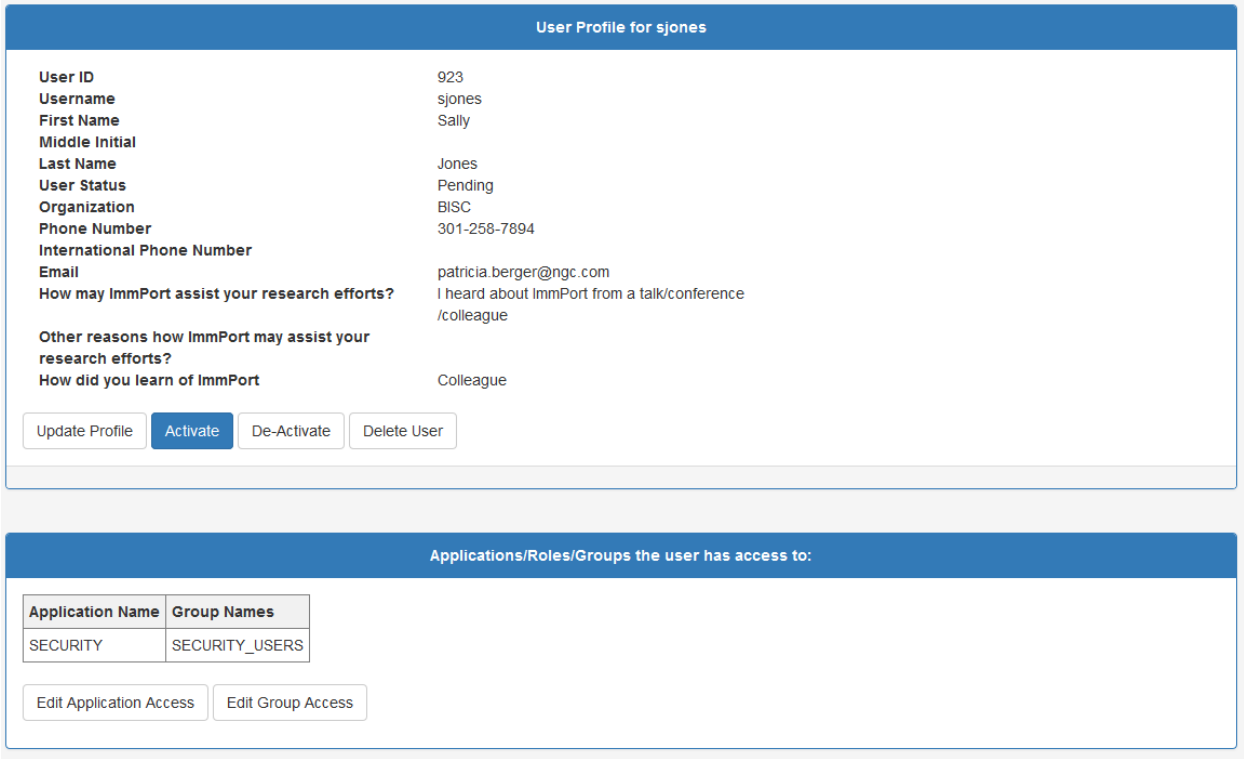
Steps:

1. The administrator clicks on the Create User menu link in the Security Admin Application. The "**Create New User**" screen is displayed.
2. The administrator enters the user profile data**.**
3. The administrator selects the required applications for the user to have access.
4. The administrator clicks on Create User button.
5. The system creates a user in the system with Pending Status. This means the user is still not validated.
6. The system assigns the default roles of the specified Applications to the user and the default User Role.
7. The system creates a user in the ImmPort 2 database with Pending status. There is a trigger on the BISC_SECURITY.USER_INFO to populate the table in the DEVELOPER.USER_INFO schema. Please refer to the trigger TR_AIU_BISC_USER_INFO.
8. A unique verification code is created for the user and the status is set to "User token has been sent to the user and is pending verification.
9. An email is created with a link which contains the verification token and is sent to the email address registered on the account.
10. The system displays a message indicating that the user has been sent an email containing a link. The user will need to click the link to confirm his registration and summary of his profile.
11. The user receives a confirmation email with a link to create his password.
12. The user clicks on the link and is redirected to create a password.
13. The user enters a password and confirms the password then clicks “Save Password”.
14. The system sets the verification code to the status "User is verified" and the user account is activated.
15. The system displays a message indicating the password has been successfully set.
16. The user can then login to the original application with their username and password.

1.1.2.3 Assign Roles to the new user


Create New User For ImmPort
A user account is created with the following information. A message will be sent to the user on the email account to set his password on the account.
User ID 923
Username sjones
First Name Sally
Middle Initial
Last Name Jones
Organization BISC
Phone Number 301-258-7894
International Phone Number
Email patricia.berger@ngc.com
How may ImmPort assist your research efforts? I heard about ImmPort from a talk/conference /colleague
Other reasons how ImmPort may assist your research efforts?
How did you learn of ImmPort Colleague
List of applications requested access for
Continue to assign roles to the user
User Profile for sjones
User ID 923
Username sjones
First Name Sally
Middle Initial
Last Name Jones
User Status Pending
Organization BISC
Phone Number 301-258-7894
International Phone Number
Email patricia.berger@ngc.com
How may ImmPort assist your research efforts? I heard about ImmPort from a talk/conference /colleague
Other reasons how ImmPort may assist your research efforts?
How did you learn of ImmPort Colleague
Update Profile
Activate
De-Activate
Delete User
Applications/Roles/Groups the user has access to:
Application Name
Group Names
Edit Application Access
Edit Group Access





1.1.2.4 Assign Roles to the new user Use Case

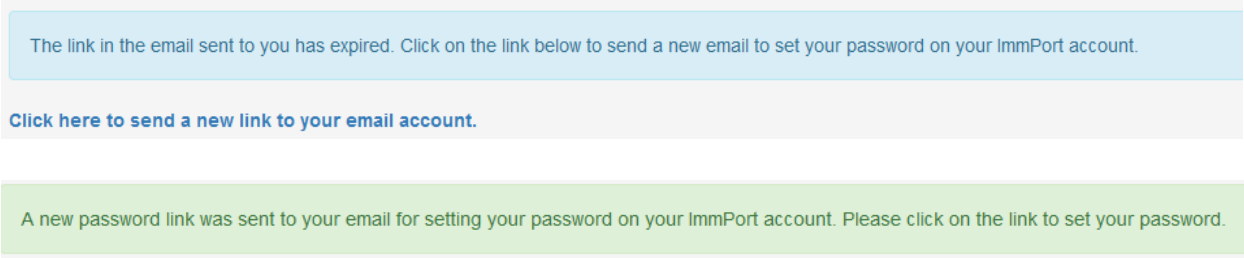
Actor: A user with the SECURITY_USER ROLE

Pre-Conditions: The actor has access to the Security Application
Post-Conditions: A user is created in the system with a default User Role and the default Roles of the Applications.

1. The administrator will click on the "Continue to assign roles to the user" button.

2. The "**Search User**" screen is displayed with the user details, applications, groups, and roles are assigned. The administrator has the ability to modify the user's details, applications, groups and roles.
3. The administrator will click on the "Edit Application Access" button then select and move the applications to the selected column.
4. The administrator will click the "Save" button to save the request or "Cancel" button to cancel the request.

1.1.2.5 Email Activation Link has expired



1.1.2.6 Email Activation Link has expired Use Case

Actor: A user with a PENDING_USER ROLE

Pre-Conditions: The actor has access to the Security Application
Post-Conditions: A user is created in the system with a default User Role and the default Roles of the Applications.

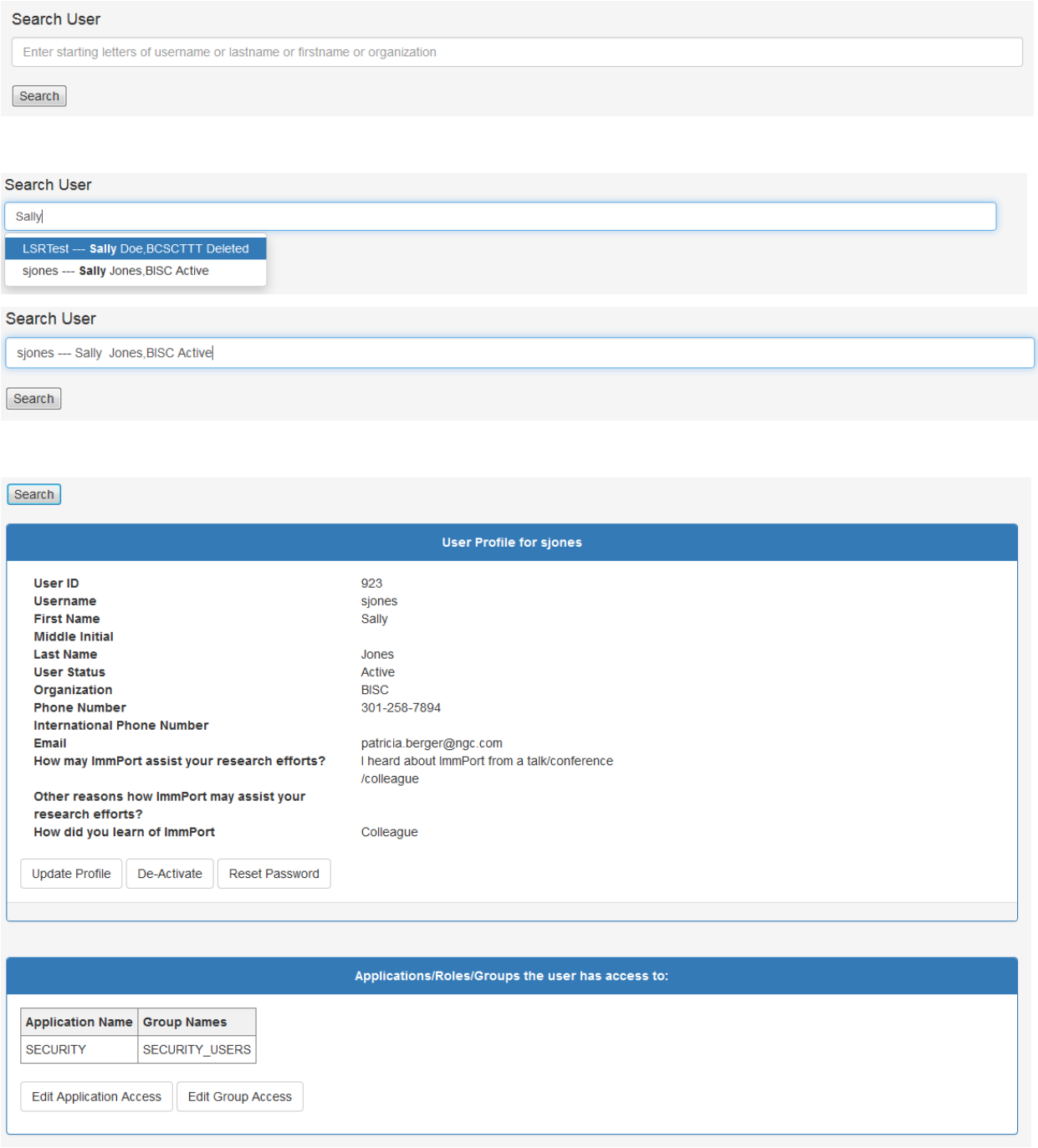
1. The user clicks on the email link after the configurable expiration period.
2. The system displays a message stating the email link has expired and a new link is provided to receive a new email with a new activation and create password link.
3. When the user clicks on the link, the system sends an email and displays a message stating an email has been sent.

Business Rules:

- The Email Address and Login Name will be used to avoid duplication of the users in the database.
- The business rule for the Use Case Register User also applies.
- The password rules are
    - The password rules be:
        - The password must contain a minimum of 8 characters.
        - Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.

1.1.2.7 Search Users

The search user depicts the events for an administrator searching a user account based on certain criteria. After the search, the user may view/update more details about the selected user.



1.1.2.8 Search Users Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged in to the Security Admin Application**.**

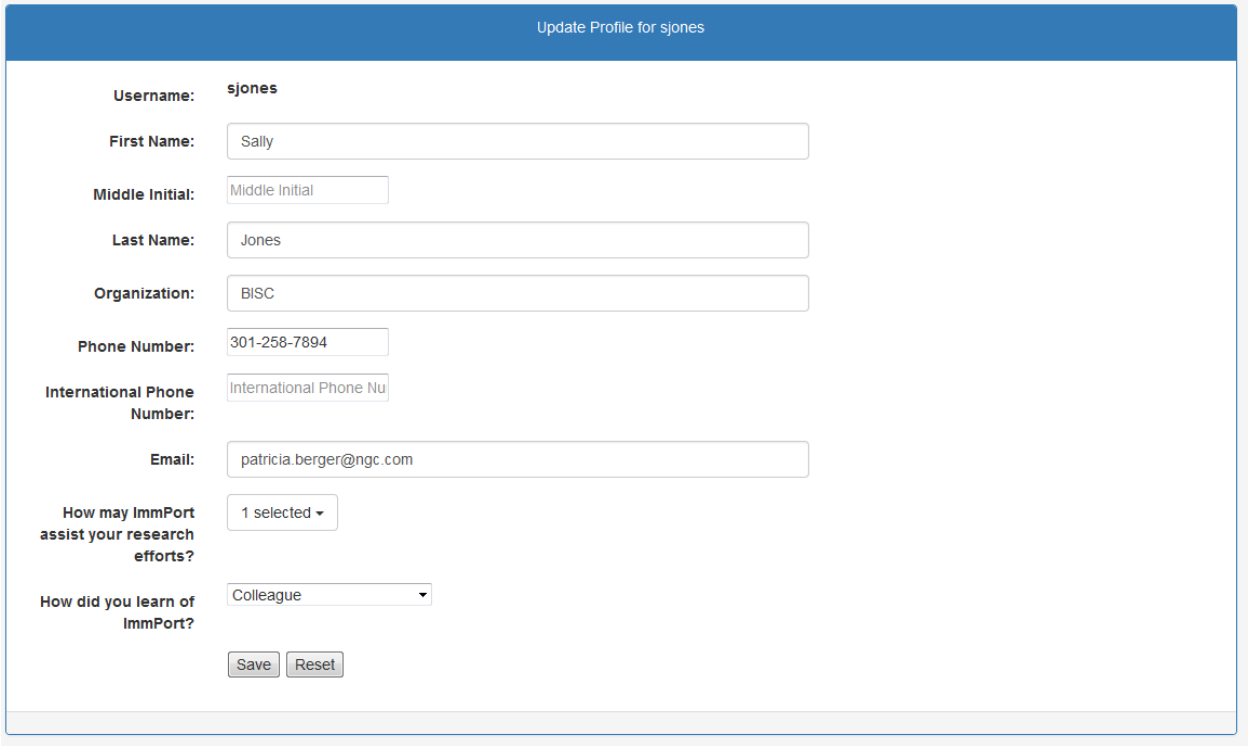
Post-Conditions: A list of users that match the criteria is displayed to the actor.

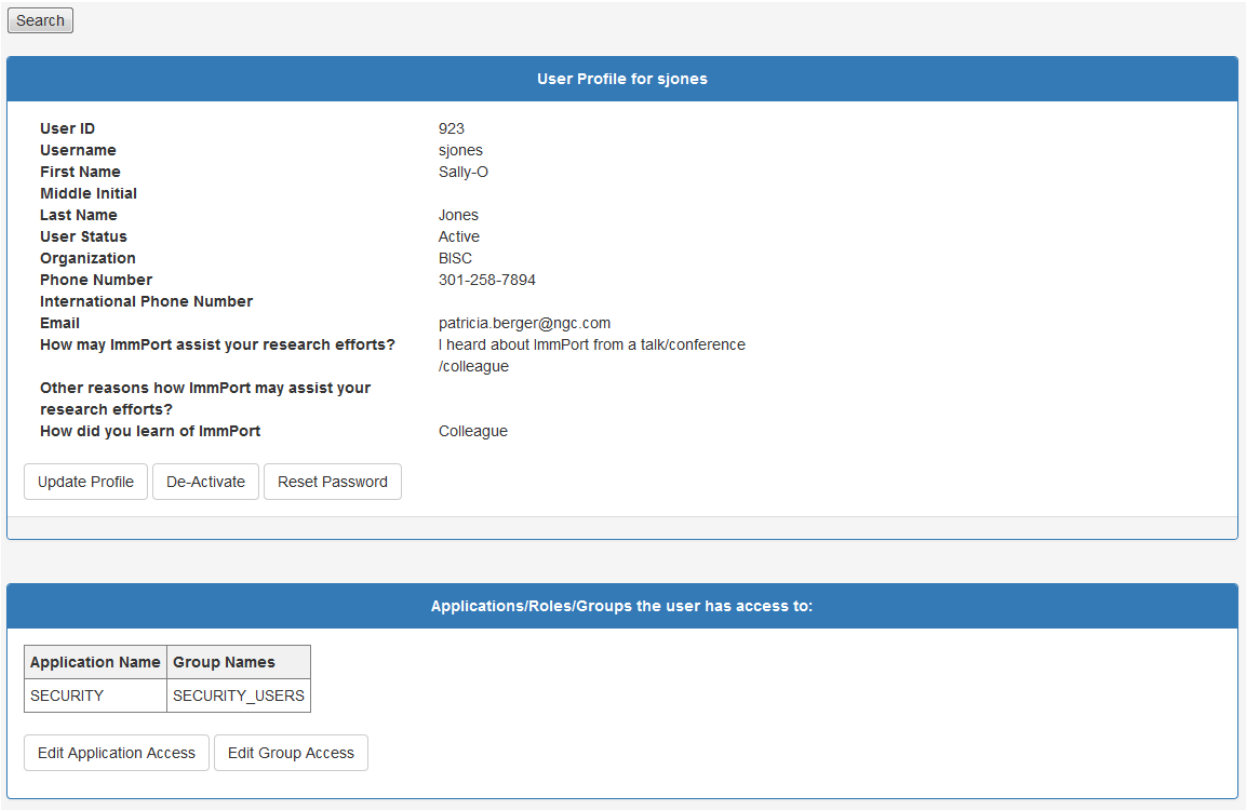
Steps:

1. The user clicks the Search User menu link in the Security Application or Search User from the ImmPort 2 Application.
2. The "**Search User**" screen is displayed.
3. The user enters the search criteria. The user can enter a few letters of the username or first name or middle name or last name or organization or status.
4. The system finds all the users matching the letters in any of the above mentioned fields.
5. The user can select a particular user from the dropdown and click on the enter button. The "**User Detail**" screen is displayed.

1.1.2.9 Update Profile

The update user depicts the events for an administrator updating a user account. Appropriate error messages are displayed if errors are encountered.





1.1.2.10 Update Profile Use Case

Actor: A user with Admin Role.

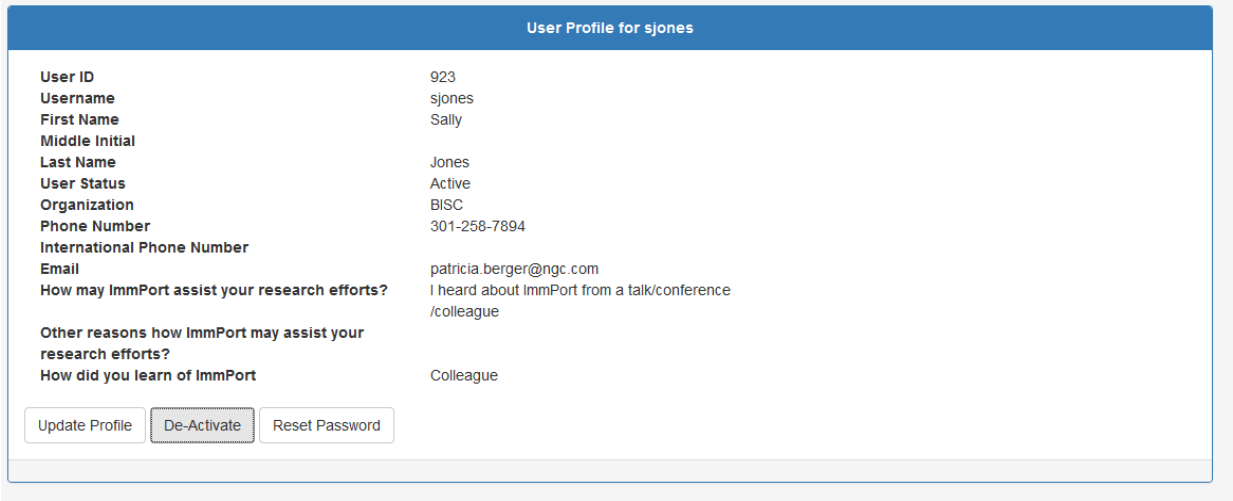
Pre-Conditions: The user is logged in to the Security Admin Application**.**

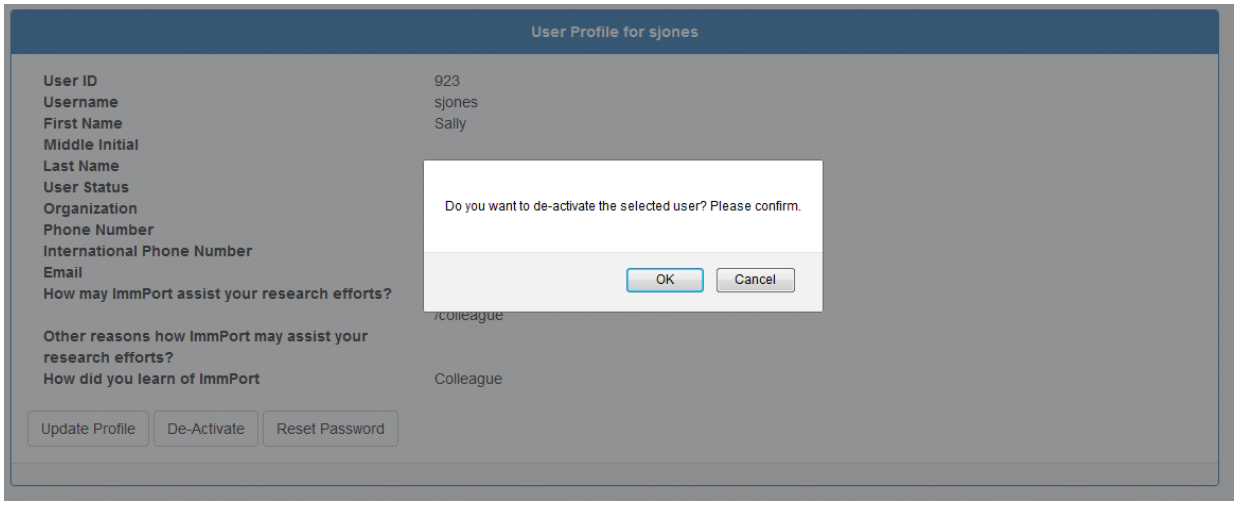
Post-Conditions: A user's profile will be updated.

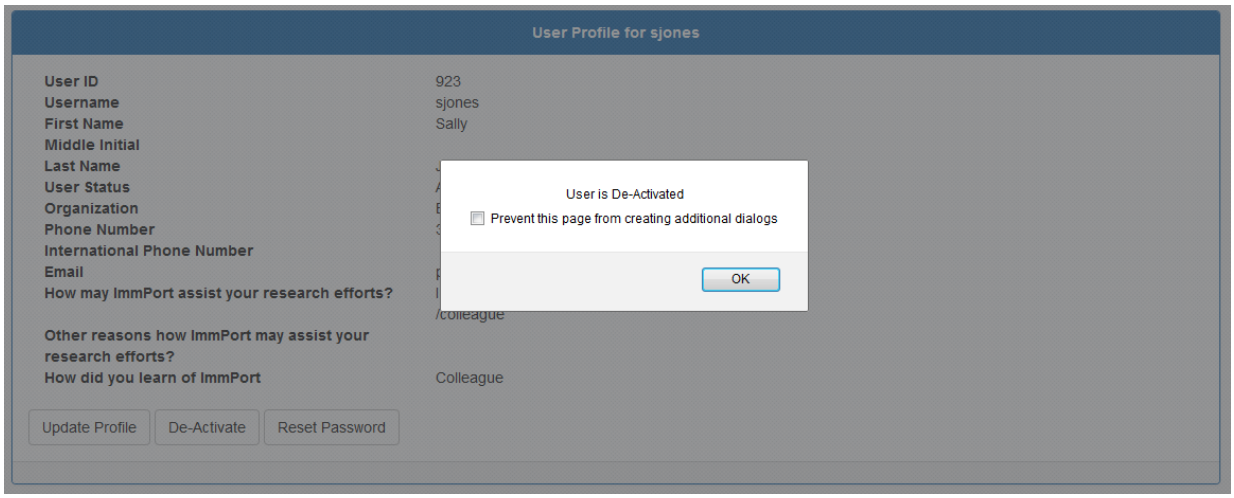
1. The administrator clicks on the Update Profile Button. The Update Profile screen is displayed and admin makes the necessary modifications and clicks on the Save button.
2. The system displays the User Details screen with the changed data.

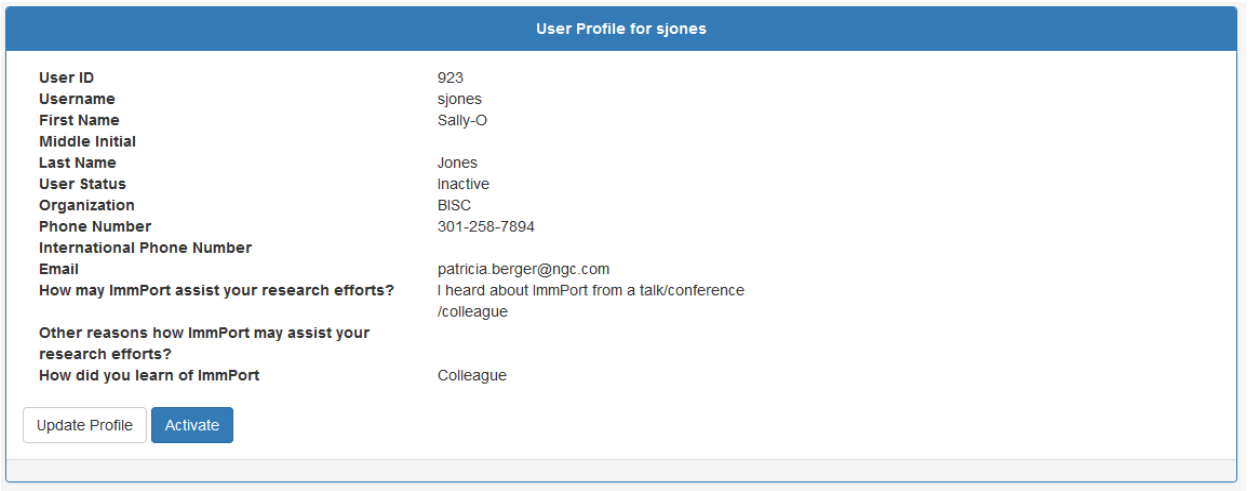
1.1.2.11 Deactivate User

The Deactivate depicts the events for deactivating a user account. Appropriate error messages are displayed if errors are encountered.


User Profile for sjones
User ID 923
Username sjones
First Name Sally
Middle Initial
Last Name Jones
User Status Active
Organization BISC
Phone Number 301-258-7894
International Phone Number
Email patricia.berger@ngc.com
How may ImmPort assist your research efforts? I heard about ImmPort from a talk/conference /colleague
Other reasons how ImmPort may assist your research efforts?
How did you learn of ImmPort Colleague
Update Profile
De-Activate
Reset Password


User Profile for sjones
User ID 923
Username sjones
First Name Sally
Middle Initial
Last Name
User Status
Organization
Phone Number
International Phone Number
Email
How may ImmPort assist your research efforts?
Other reasons how ImmPort may assist your research efforts?
How did you learn of ImmPort Colleague
Update Profile
De-Activate
Reset Password
Do you want to de-activate the selected user? Please confirm.
OK
Cancel


User Profile for sjones
User ID 923
Username sjones
First Name Sally
Middle Initial
Last Name
User Status
Organization
Phone Number
International Phone Number
Email
How may ImmPort assist your research efforts?
Other reasons how ImmPort may assist your research efforts?
How did you learn of ImmPort Colleague
Update Profile
De-Activate
Reset Password
User is De-Activated
Prevent this page from creating additional dialogs
OK



1.1.2.12 Deactivate User Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged in to the Security Admin Application**.**

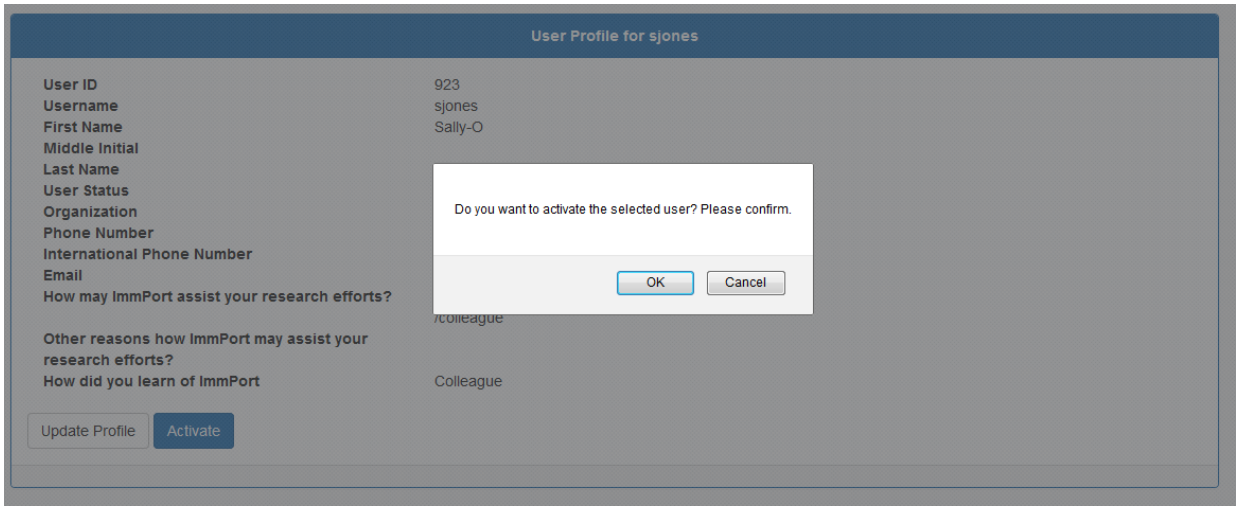
Post-Conditions: A user is deactivated from the system.

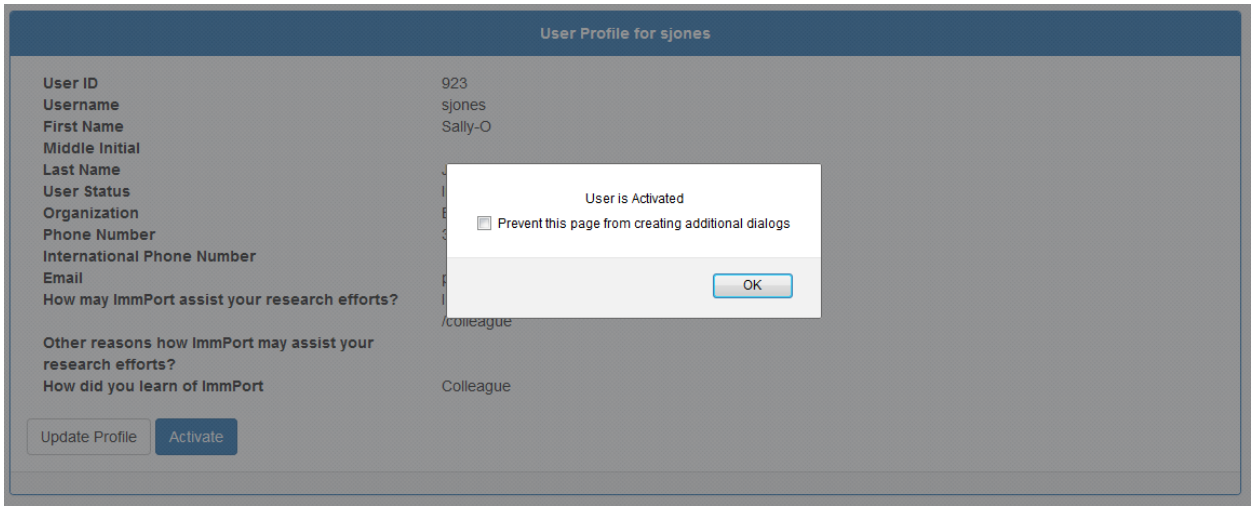
Steps:

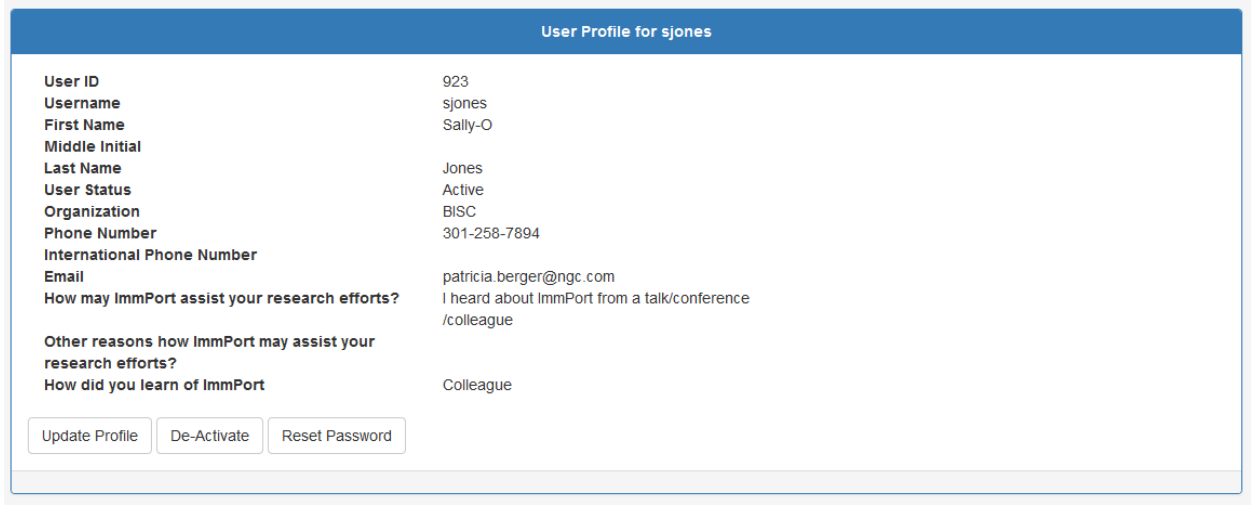
1. The admin clicks on the De-Activate Button. The De-activate button is only displayed if the user status is Pending or Active.
2. The system displays a message that the user is de-activated and the Status is changed to Inactive.

1.1.2.13 Activate User

The activate user depicts the events for activating a user account that has been deactivated in the past. Appropriate error messages are displayed if errors are encountered.


User Profile for sjones
User ID 923
Username sjones
First Name Sally-O
Middle Initial
Last Name
User Status
Organization
Phone Number
International Phone Number
Email
How may ImmPort assist your research efforts?
Other reasons how ImmPort may assist your research efforts?
How did you learn of ImmPort Colleague
Do you want to activate the selected user? Please confirm.
OK
Cancel
Update Profile
Activate


User Profile for sjones
User ID 923
Username sjones
First Name Sally-O
Middle Initial
Last Name
User Status
Organization
Phone Number
International Phone Number
Email
How may ImmPort assist your research efforts?
Other reasons how ImmPort may assist your research efforts?
How did you learn of ImmPort Colleague
User is Activated
Prevent this page from creating additional dialogs
OK
Update Profile
Activate


User Profile for sjones
User ID 923
Username sjones
First Name Sally-O
Middle Initial
Last Name Jones
User Status Active
Organization BISC
Phone Number 301-258-7894
International Phone Number
Email patricia.berger@ngc.com
How may ImmPort assist your research efforts? I heard about ImmPort from a talk/conference /colleague
Other reasons how ImmPort may assist your research efforts?
How did you learn of ImmPort Colleague
Update Profile
De-Activate
Reset Password

1.1.2.14 Activate User Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged in to the Security Admin Application**.**

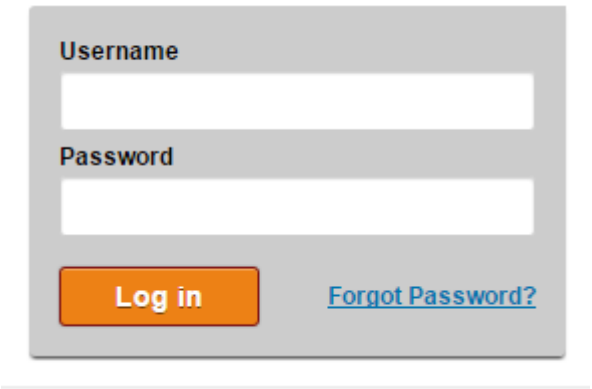
Post-Conditions: A user will be activated in the system.

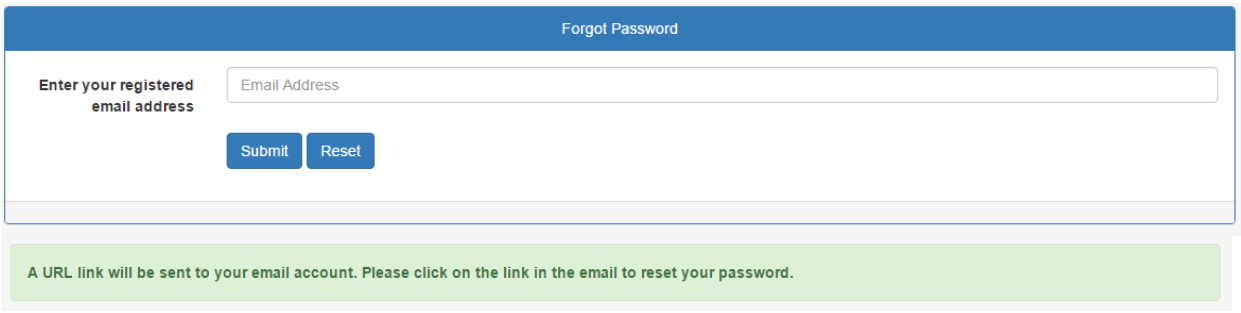
Steps:

1. The admin clicks on the Activate Button. The Activate button is only displayed if the user status is Pending or Inactive.
2. The system displays a message that the user is activated and the Status is changed to active.

1.1.2.15 Reset Password

The reset password depicts the events for resetting a user's account when the user has forgotten their password. Appropriate error messages are displayed if errors are encountered.

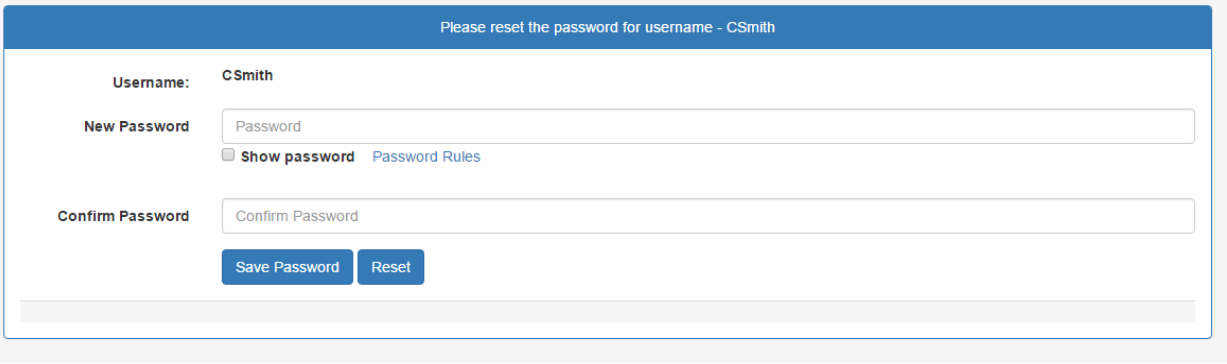


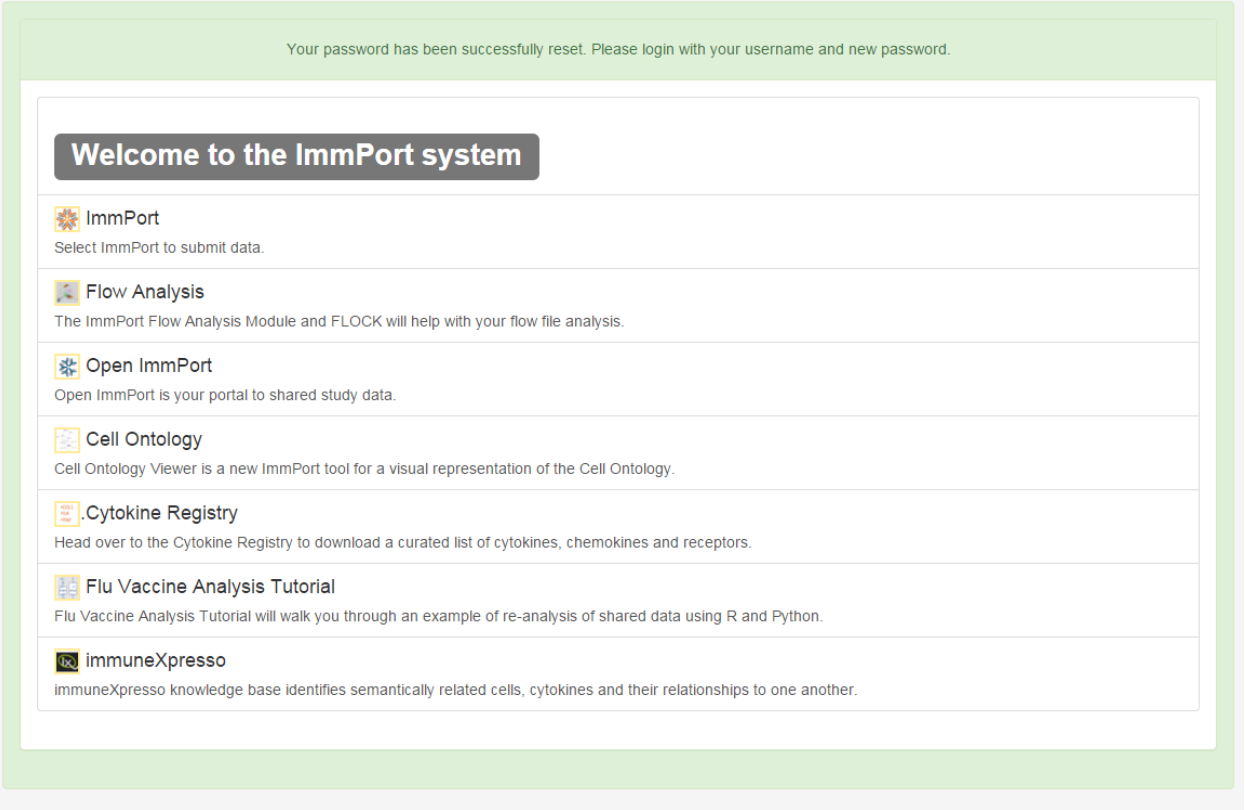


Dear Cierra Smith,

The link below will allow you to reset the password on your ImmPort Account.
Click here to reset your password

This is an automated message. Please do not reply to this email, but contact BISC_HELPDESK@mail.nih.gov if you have any questions.





Dear Cierra Smith,

This email is sent to notify you that the password on the ImmPort account associated to this email has been changed.

This is an automated message. Please do not reply to this email, but contact BISC_HELPDESK@mail.nih.gov if you have any questions.

1.1.2.16 Reset Password Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged in to the Security Admin Application**.**

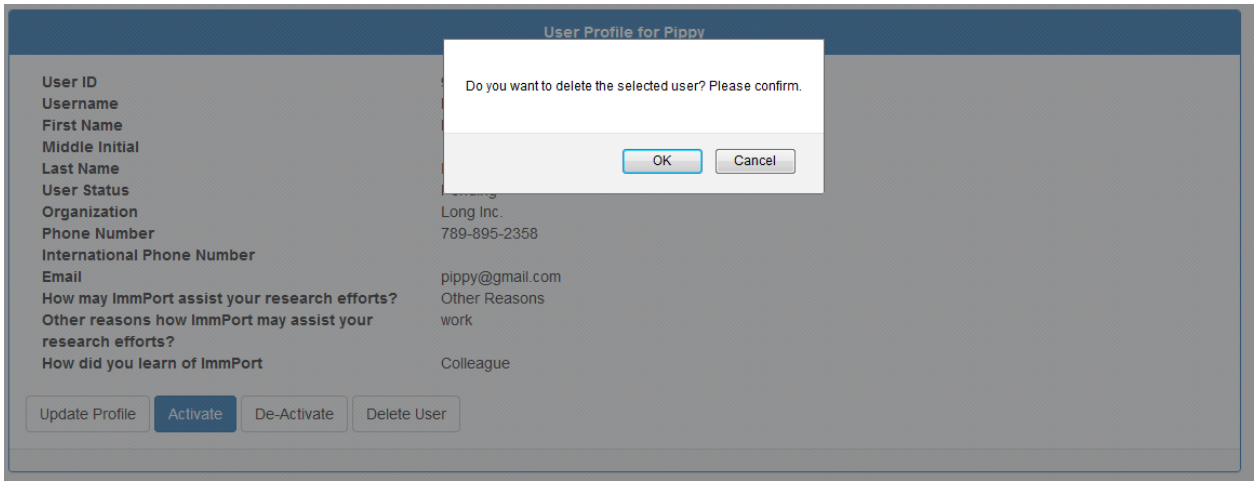
Post-Conditions: A user will reset a user's password.

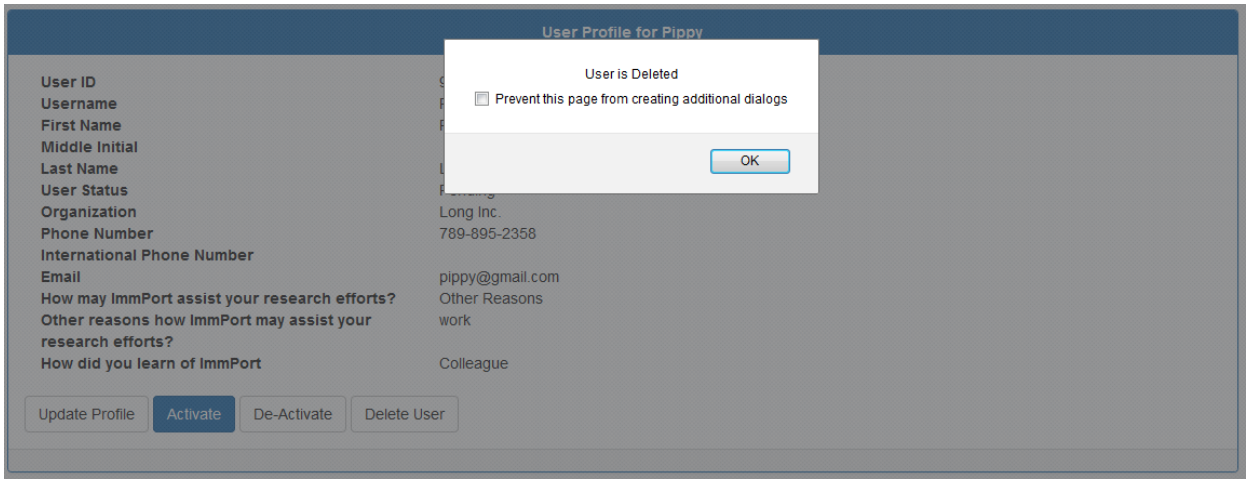
Steps:

1. The admin clicks on the Reset Password Button. The Reset Password button is only displayed if the user status is Active.
2. The system displays a message that the user has been sent a email for resetting his password and user status is changed to Pending.
3. The user clicks on the URL link on the Reset Password Email.
4. The system displays the Reset Password screen
5. The user resets his password.
6. The system displays a Success Screen.

1.1.2.17 Delete User

The delete user depicts the events for deleting a user account. Appropriate error messages are displayed if errors are encountered.





1.1.2.18 Delete User Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged in to the Security Admin Application**.**

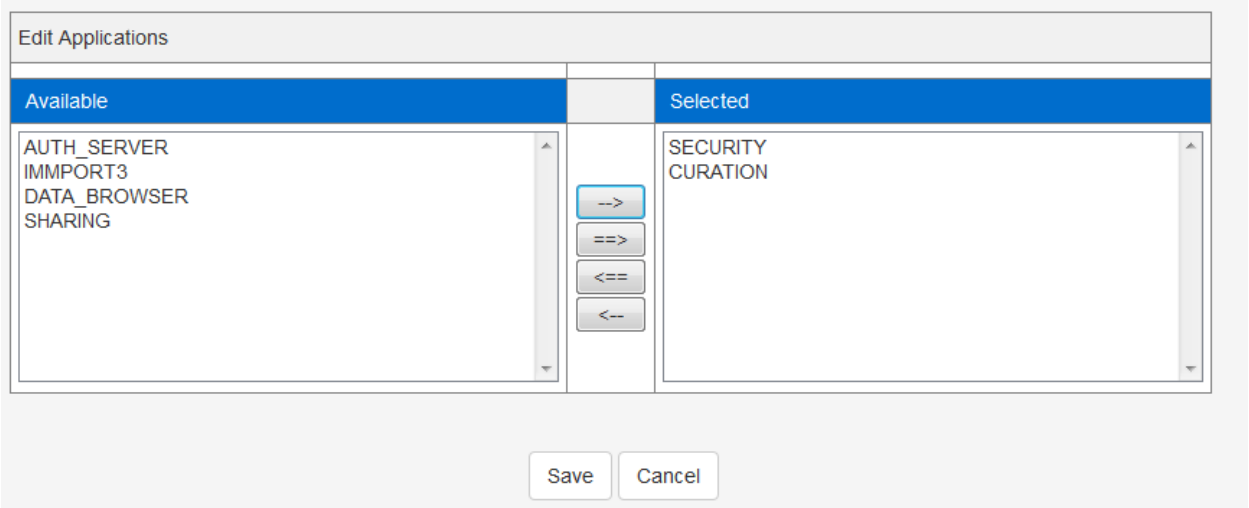
Post-Conditions: A user will delete a user's account.

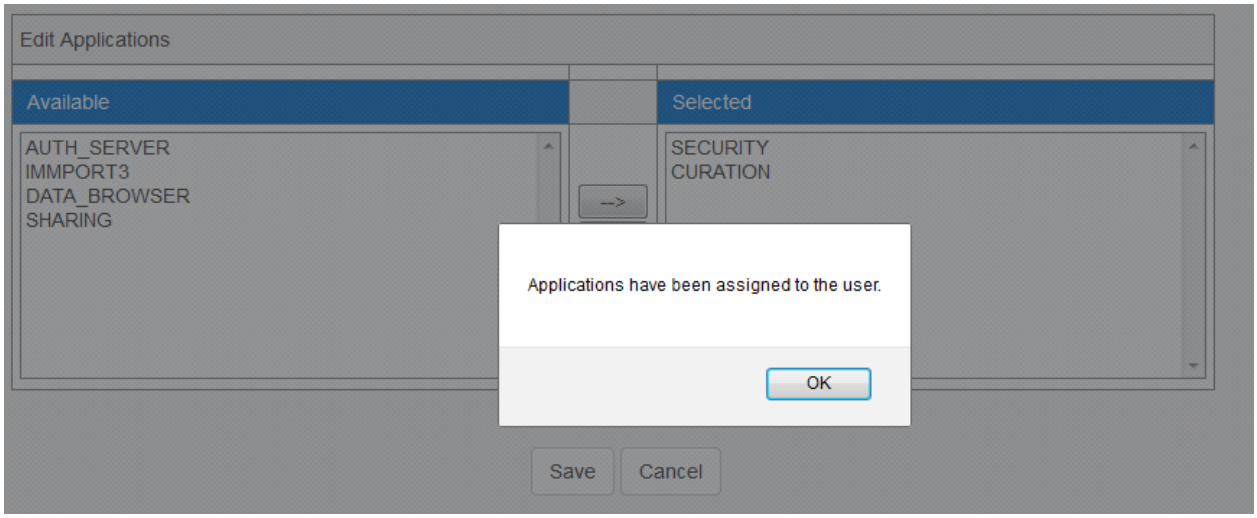
Steps:

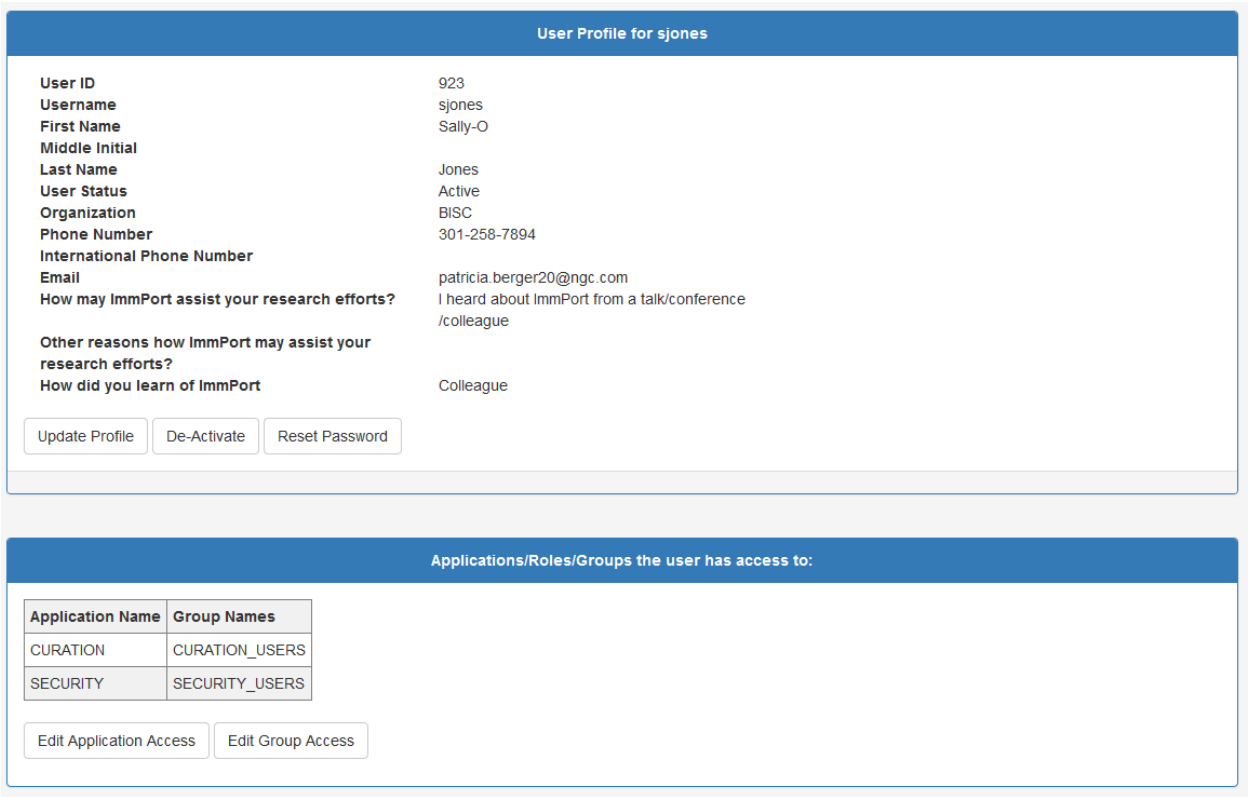
1. The admin clicks on the Delete User Button. The Delete User button is only displayed if the user is in Pending status.
2. The system deletes the user from the System and its related child elements.
3. The system displays a message that the user is deleted and the Search Screen is displayed.

1.1.2.19 Modify Application Access

Modify Application Access depicts the events for modifying application access. Appropriate error messages are displayed if errors are encountered.


Edit Applications
Available
Selected
AUTH_SERVER
IMMPORT3
DATA_BROWSER
SHARING
SECURITY
CURATION
-->
==>
<==
<--
Save
Cancel


Edit Applications
Available
Selected
AUTH_SERVER
IMMPORT3
DATA_BROWSER
SHARING
SECURITY
CURATION
-->
Applications have been assigned to the user.
OK
Save
Cancel



1.1.2.20 Modify Application Access Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged in to the Security Admin Application**.**

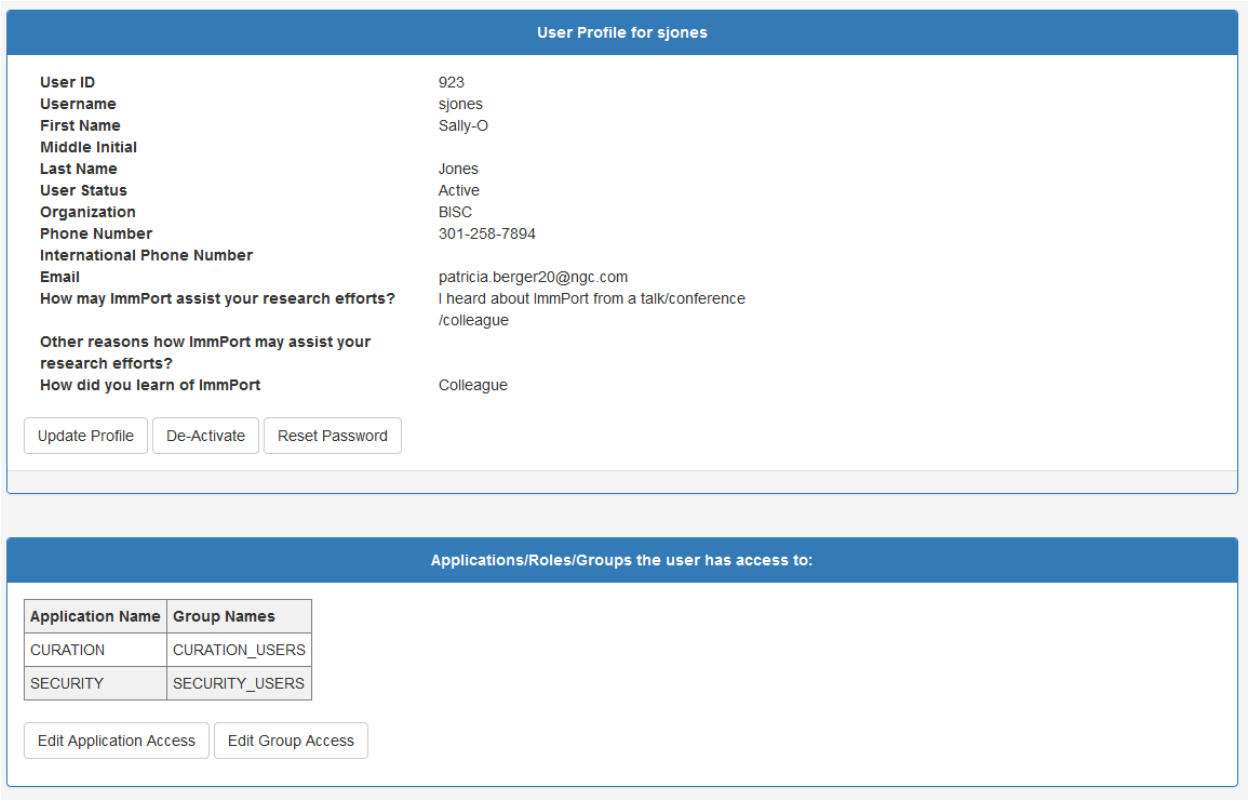
Post-Conditions: A user will have access to the appropriate application(s).

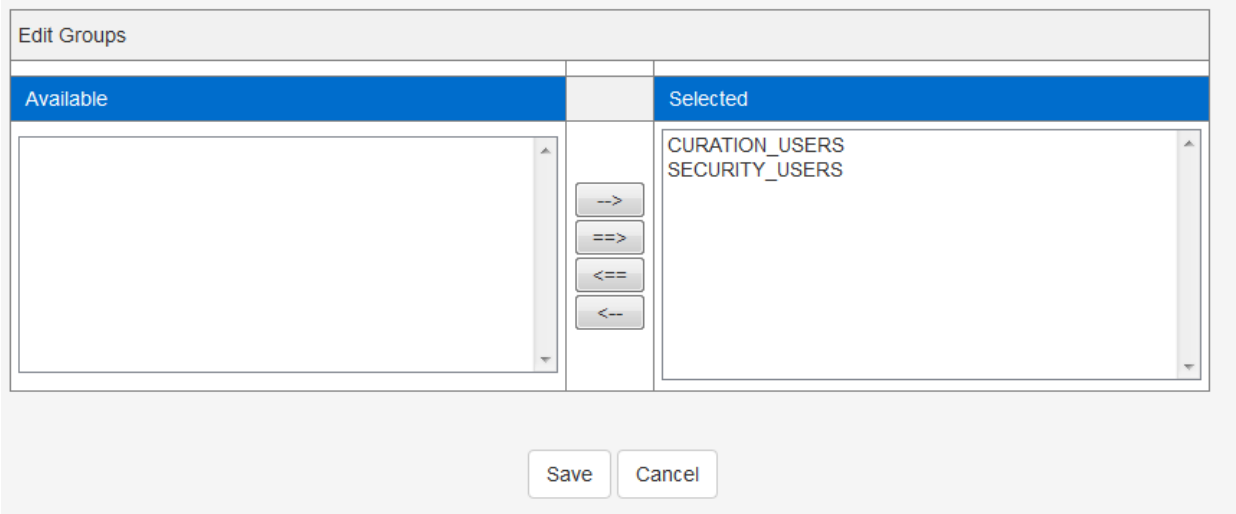
Steps:

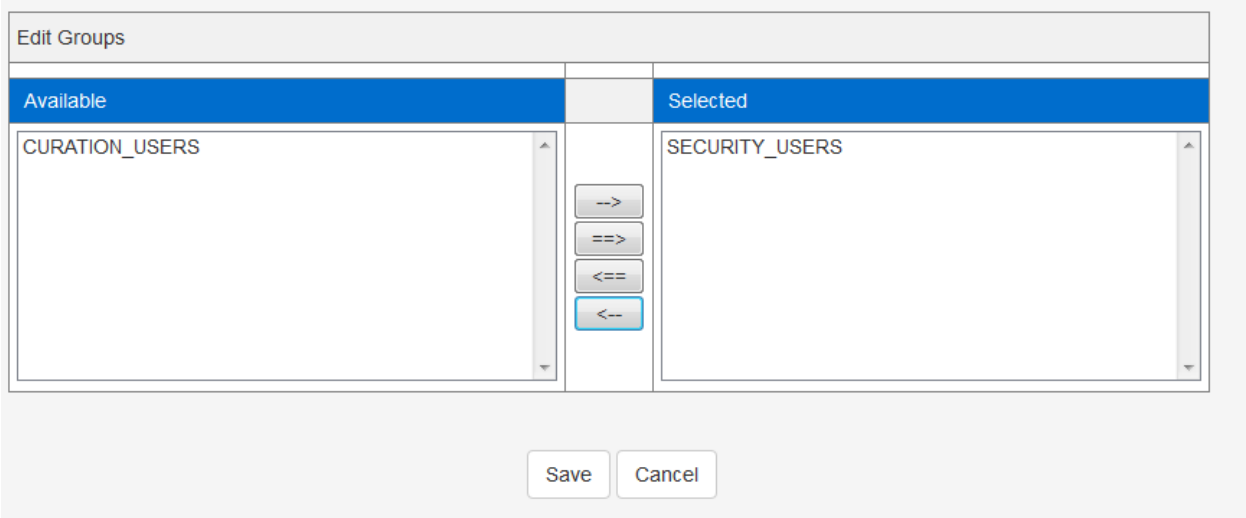
1. The admin clicks on the Edit Application Access Button.
2. The Edit Application Access screen is displayed
3. The admin can assign access to an Application by moving the Application from the Available box to the Selected box.
4. The admin can remove access to an Application by moving the Application from the Selected box to the Available box.
5. The admin user clicks on the Save button.
6. The system assigns the Application in the Selected box and it's corresponding default Group to the User.
7. The system removes access to the Applications in the Available box and it's corresponding groups from the user.

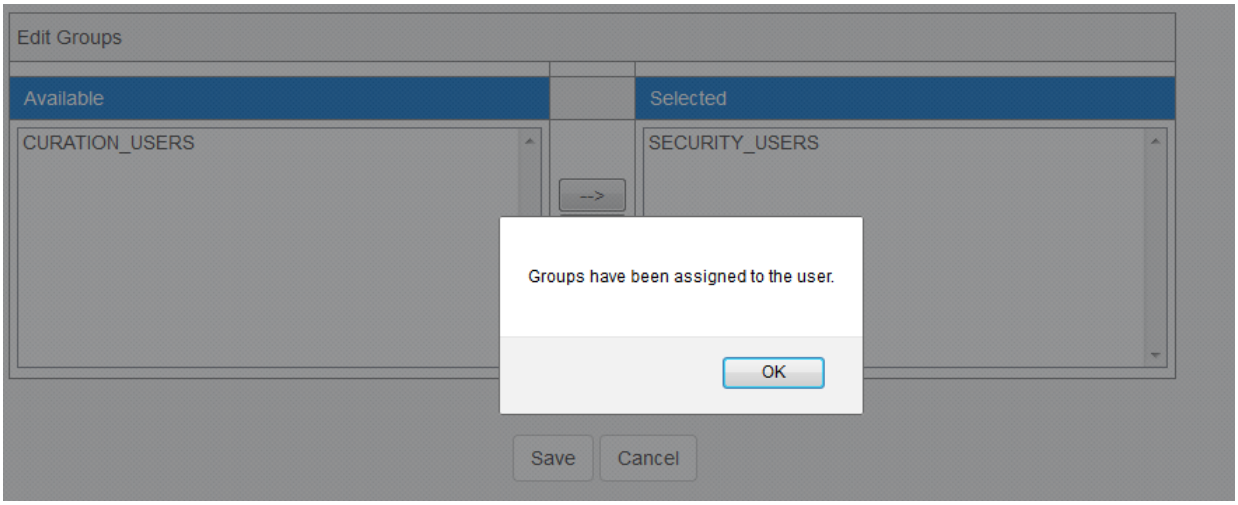
1.1.2.21 Modify Group Access

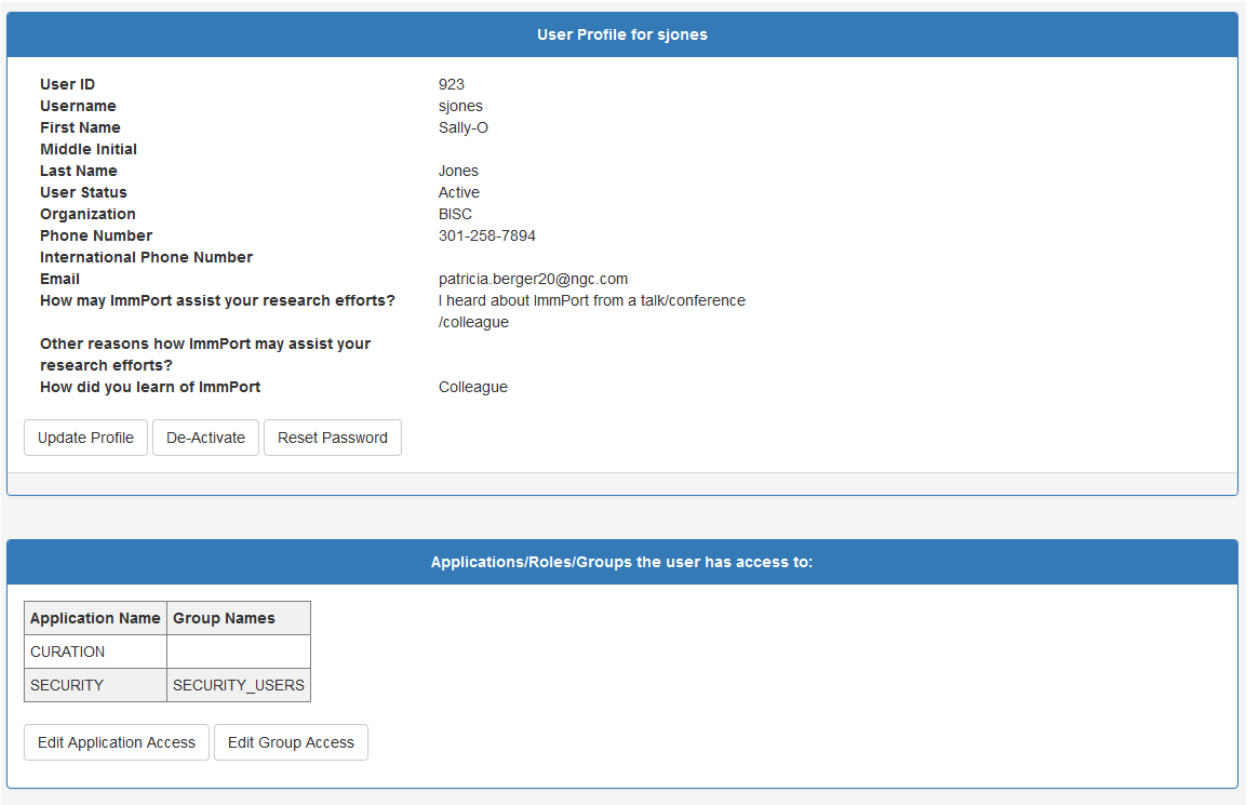
Modify Group Access depicts the events for modifying group access. Appropriate error messages are displayed if errors are encountered.






Edit Groups
Available
Selected
CURATION_USERS
SECURITY_USERS
-->
==>
<==
<--
Save
Cancel


Edit Groups
Available
Selected
CURATION_USERS
SECURITY_USERS
-->
Groups have been assigned to the user.
OK
Save
Cancel



1.1.2.22 Modify Group Access Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged in to the Security Admin Application**.**

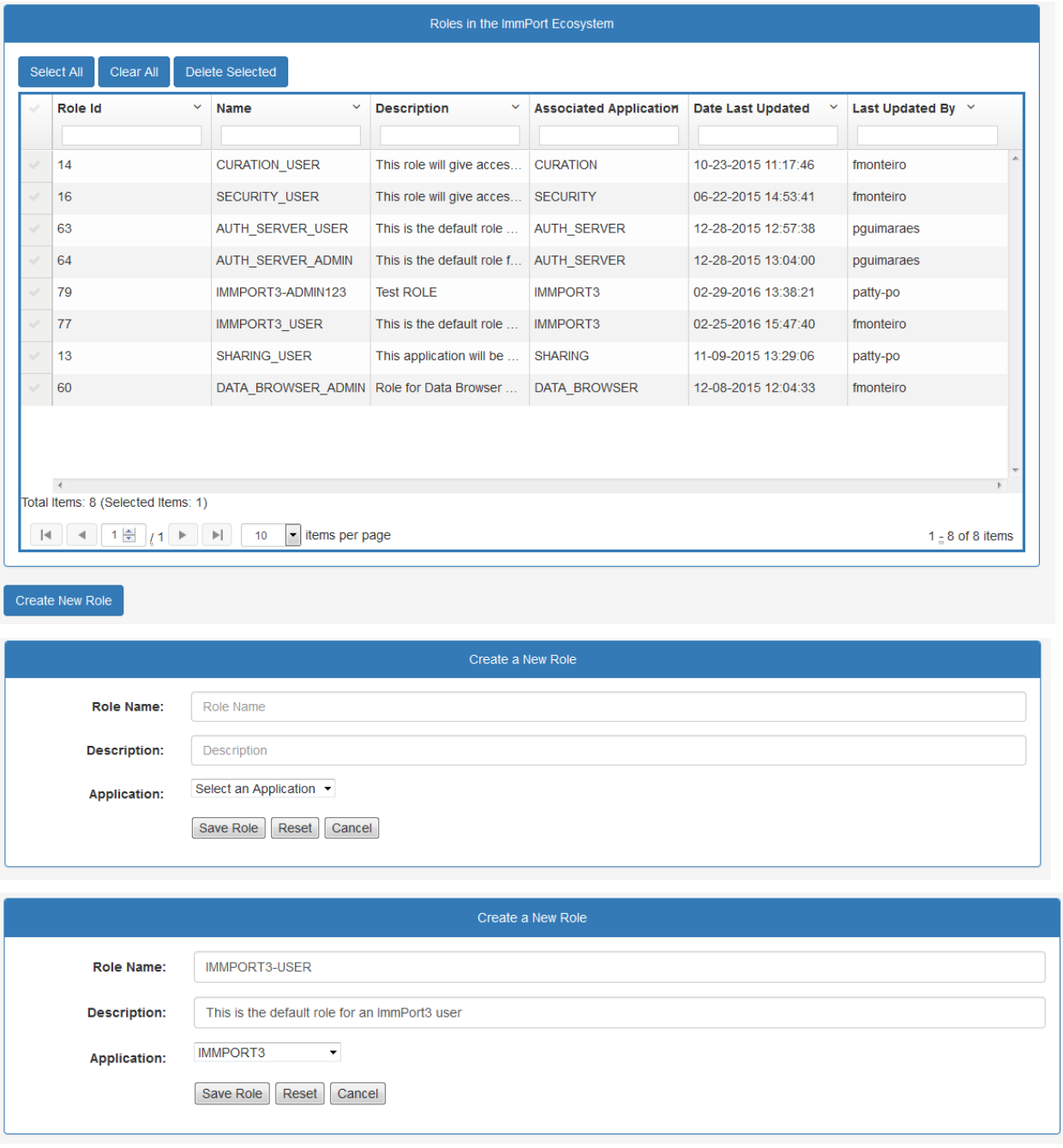
Post-Conditions: A user will have group access to the appropriate application(s).

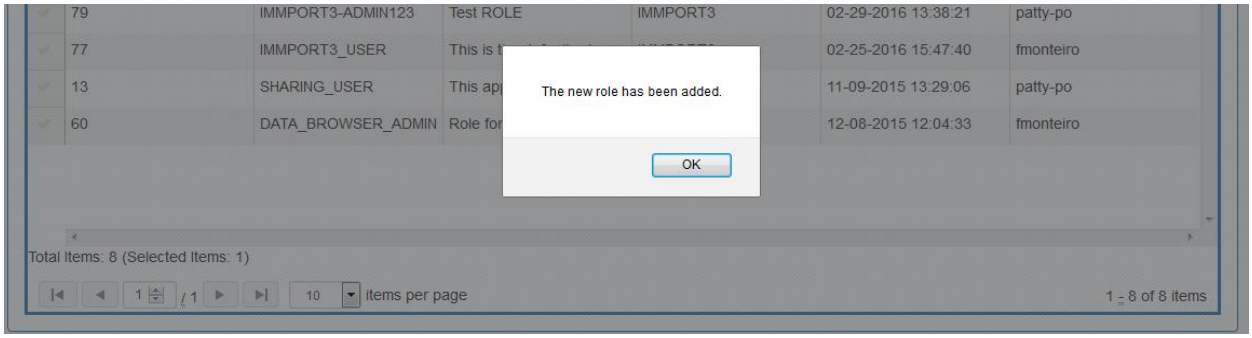
Steps:

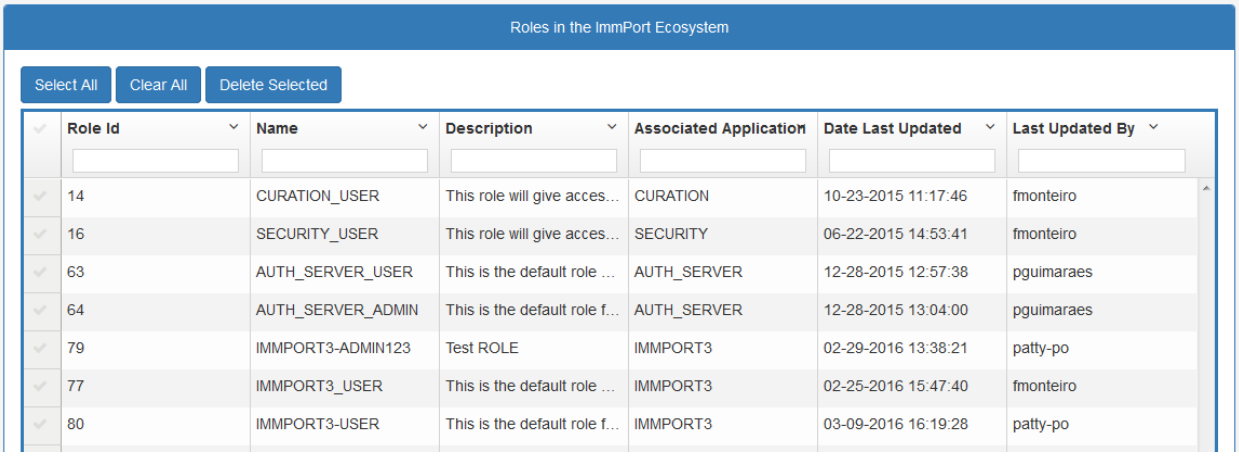
1. The admin clicks on the Edit Group Access Button.
2. The Edit Group Access screen is displayed
3. The admin can assign access to a Group by moving the Group from the Available box to the Selected box.
4. The admin can remove access to a Group by moving the Group from the Selected box to the Available box.
5. The admin user clicks on the Save button.
6. The system assigns the Groups in the Selected box to the User.
7. The system removes access to the Groups in the Available box from the user
8. The Groups are that assigned to the user are displayed against their corresponding Applications in the User Detail page.

1.1.2.23 Add a Role

Add a Role depicts the events for allowing the Admin Role to add a role in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.







1.1.2.24 Add a Role Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

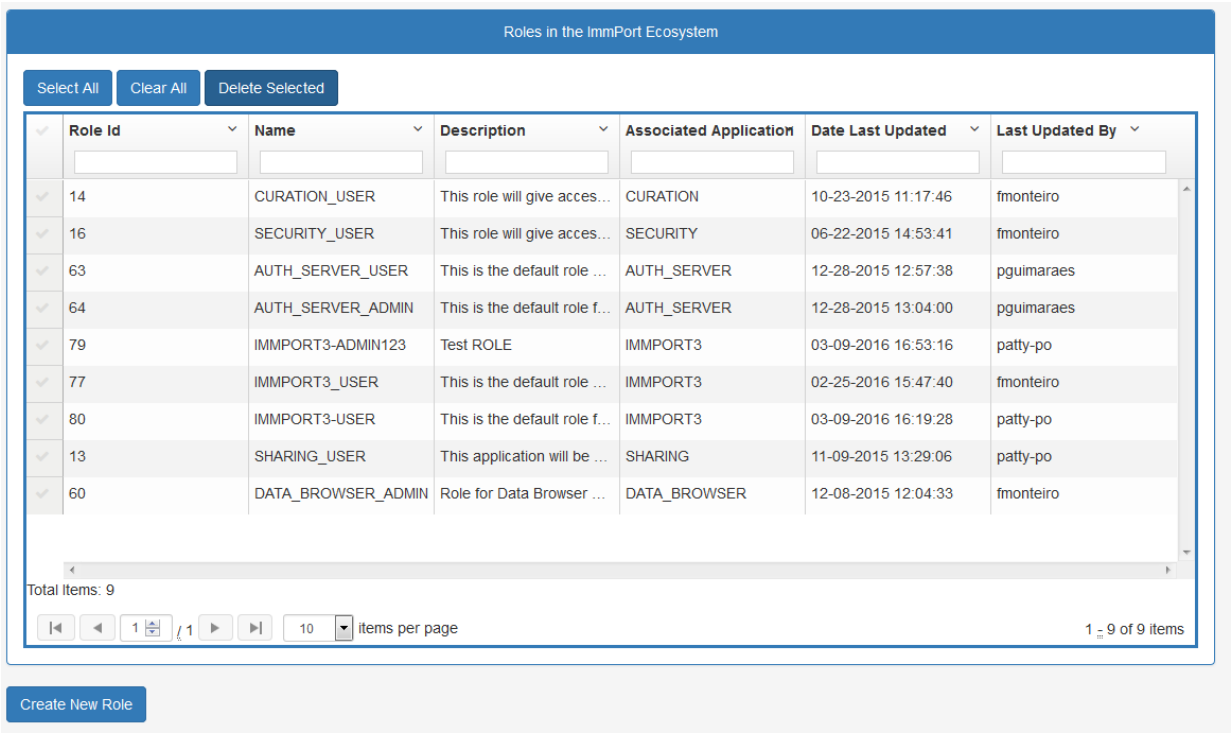
Post- Conditions: A role will be added to the ImmPort3 Ecosystem

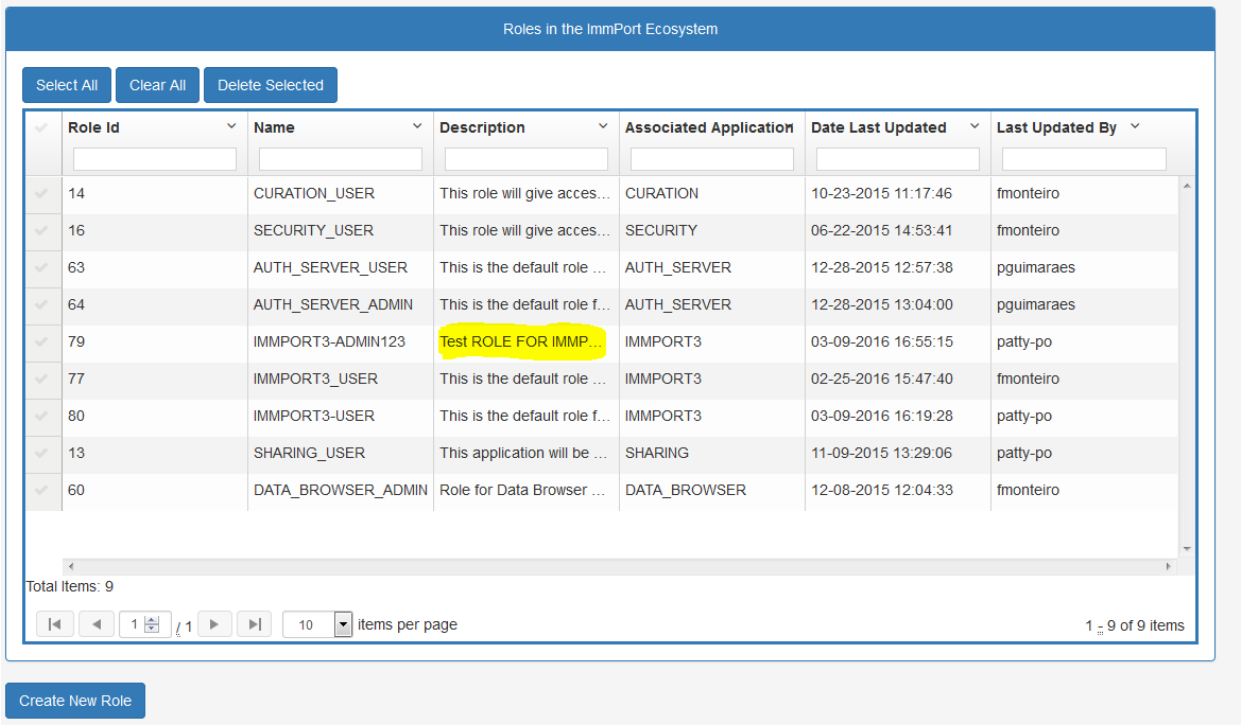
Steps:

1. The list of roles is displayed on the Role Page
2. The admin clicks on the Create New Role button.
3. The admin enters the role name, description and the application it is associated to.
4. The admin clicks Save Role.
5. The system saves the role in the database and it is displayed in the list of roles

1.1.2.25 Modify a Role

Modify a Role depicts the events for allowing the Admin Role to modify a role in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.





1.1.2.26 Modify a Role Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the Security Application.

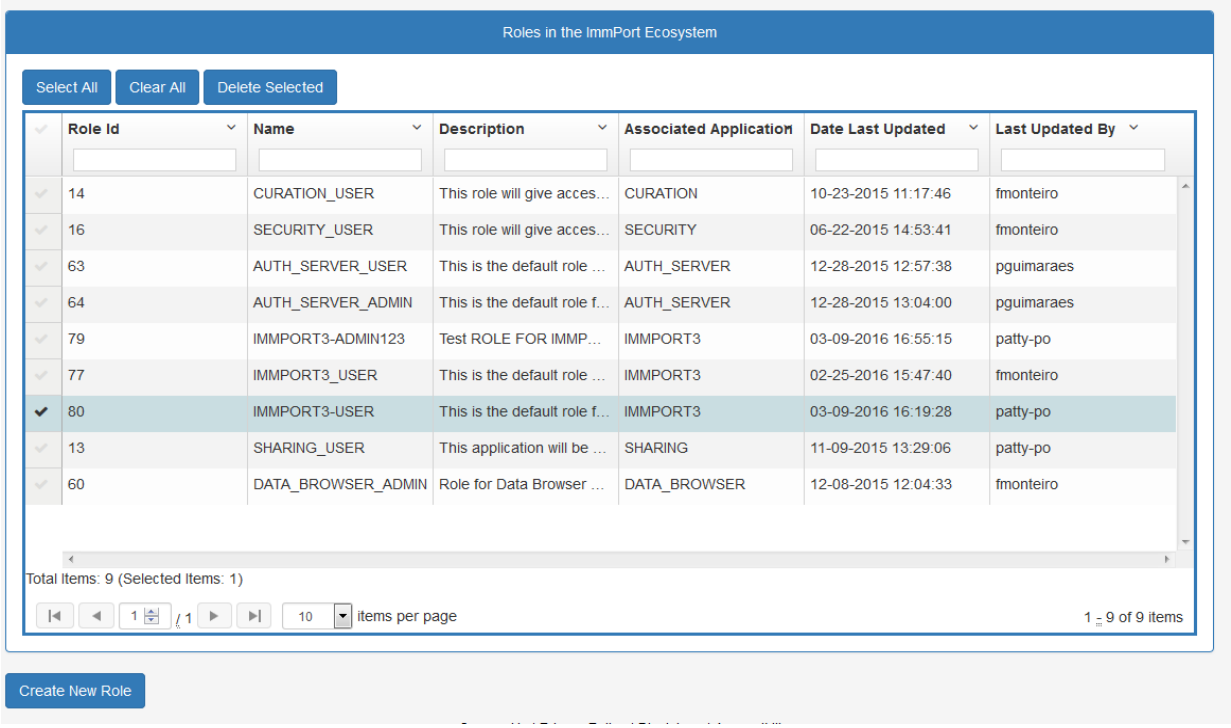
Post- Conditions: A role will be modified in the ImmPort3 Ecosystem

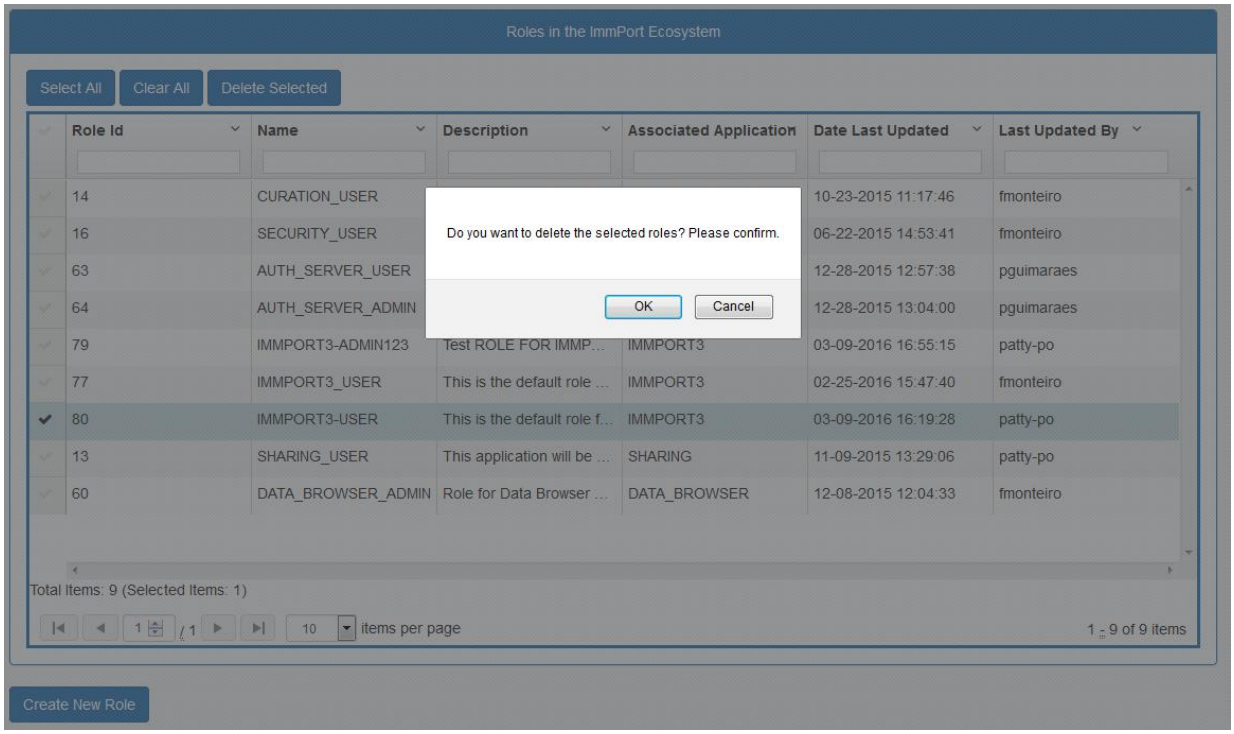
Steps:

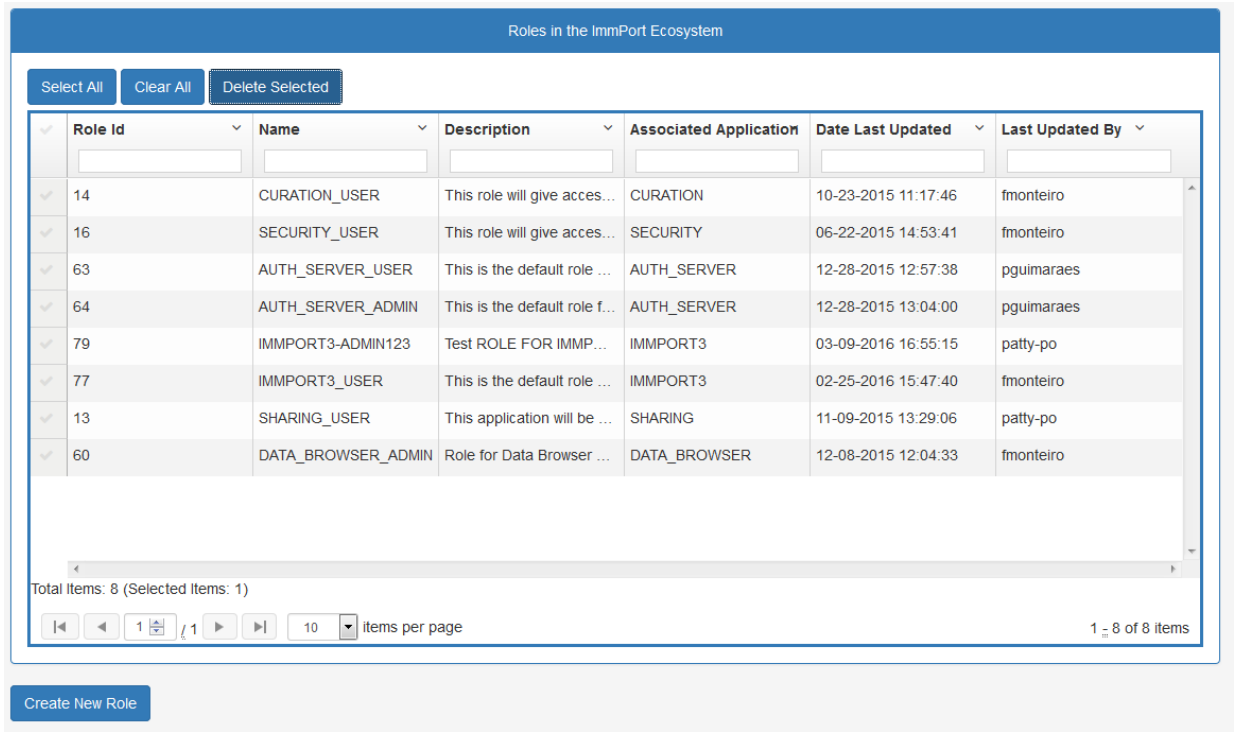
1. The admin double clicks a role name or role description.
2. The admin modifies the name or description in place.
3. The name and description is changed once the mouse looses focus on the cell.
4. The date last updated and last updated by is modified.

1.1.2.27 Delete a Role

Delete a Role depicts the events for allowing the Admin Role to delete a role in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.







1.1.2.28 Delete a Role Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

Post- Conditions: A role will be deleted in the ImmPort3 Ecosystem

Steps:

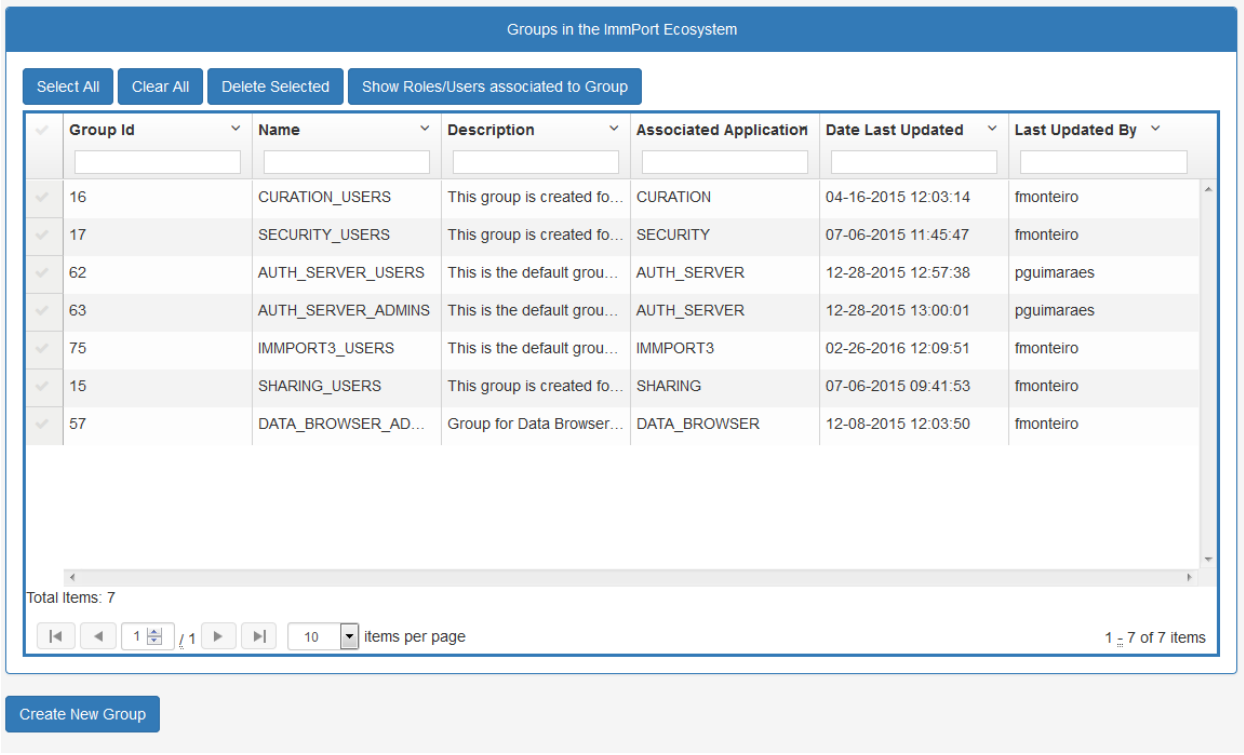
1. The admin selects a Role.
2. The admin clicks on Deleted Selected.
3. If the role is not associated to Groups and Users, the role is deleted.
4. If it is associated, a message is displayed indicating the same.

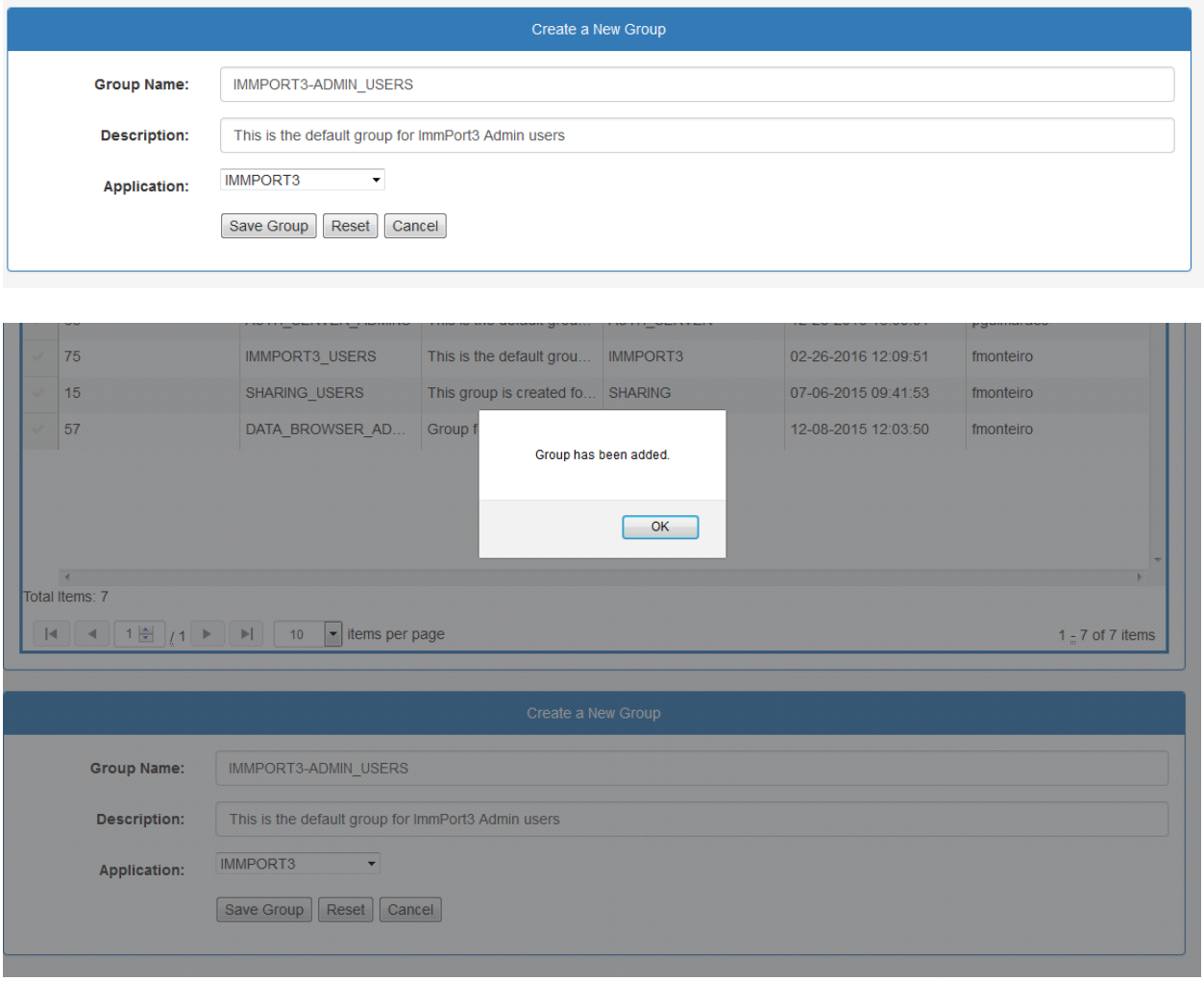
1.1.3 Manage Groups

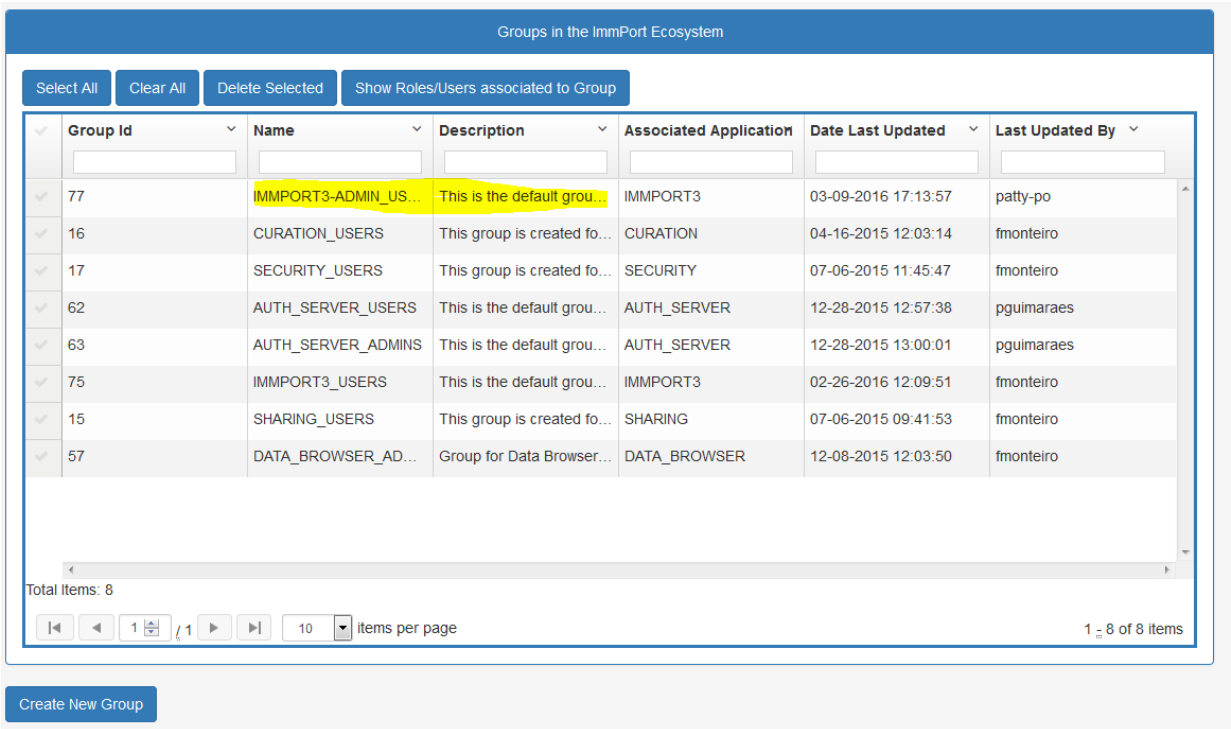
The user with Admin Role can add, delete and modify groups for the ImmPort Ecosystem.

1.1.3.1 Add a Group

Add a Group depicts the events for allowing the Admin Role to add a group in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.




Create a New Group
Group Name:
IMMPORT3-ADMIN_USERS
Description:
This is the default group for ImmPort3 Admin users
Application:
IMMPORT3
Save Group
Reset
Cancel
75
IMMPORT3_USERS
This is the default grou...
IMMPORT3
02-26-2016 12:09:51
fmonteiro
15
SHARING_USERS
This group is created fo...
SHARING
07-06-2015 09:41:53
fmonteiro
57
DATA_BROWSER_AD...
12-08-2015 12:03:50
fmonteiro
Group has been added.
OK
Total Items: 7
items per page
1 - 7 of 7 items
Create a New Group
Group Name:
IMMPORT3-ADMIN_USERS
Description:
This is the default group for ImmPort3 Admin users
Application:
IMMPORT3
Save Group
Reset
Cancel



1.1.3.2 Add a Group Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

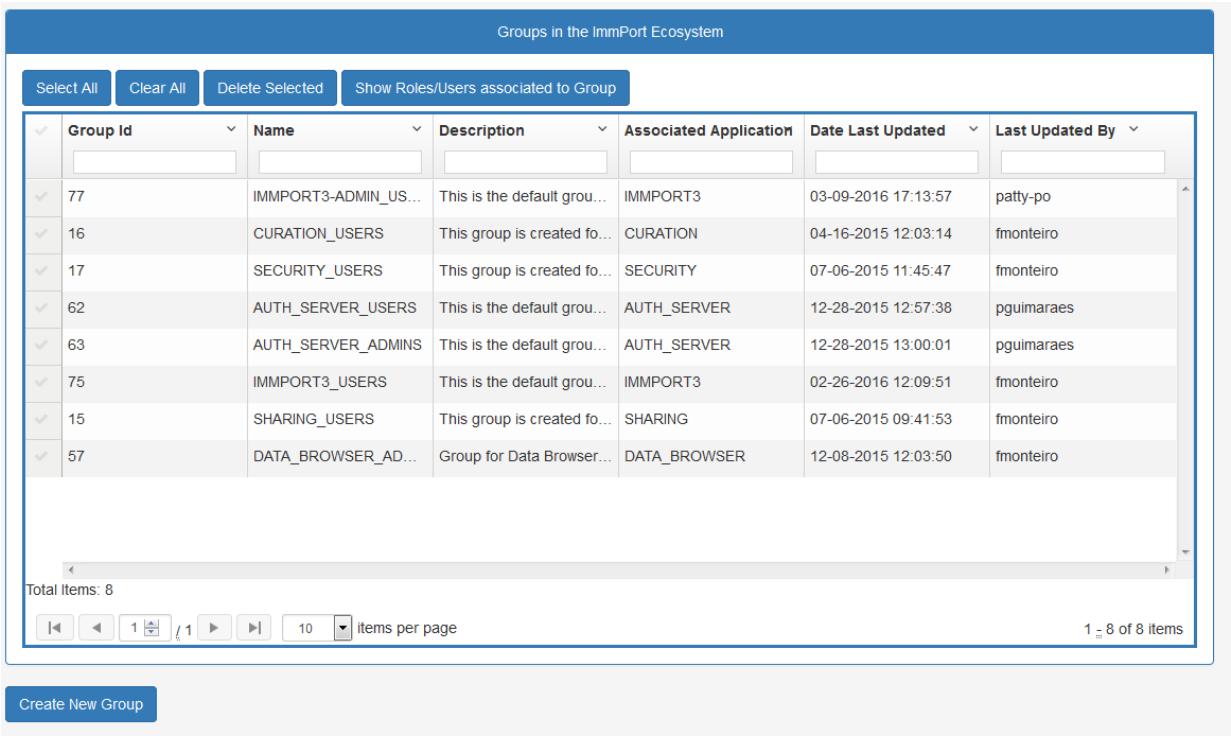
Post- Conditions: A group will be added in the ImmPort3 Ecosystem

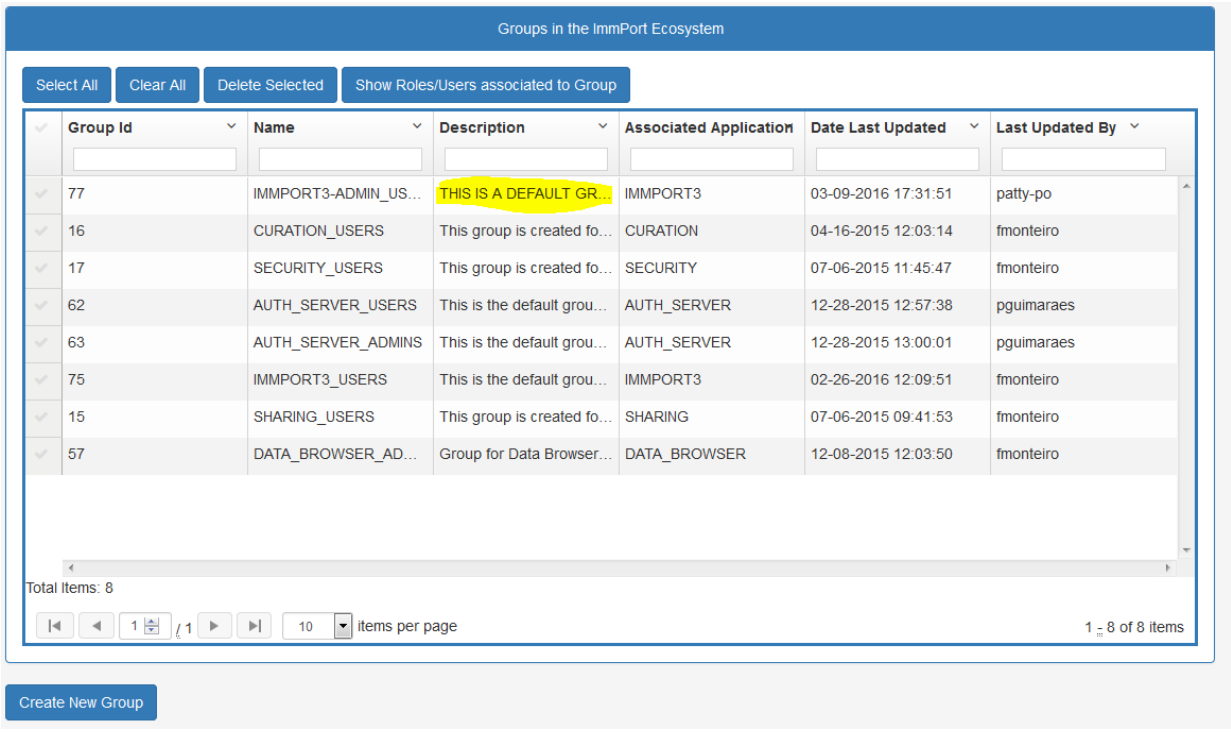
Steps:

1. The admin clicks on the Create New Group button.
2. The admin enters the group name, description and the application it is associated to.
3. The admin clicks Save Group.
4. The system saves the group in the database and it is displayed in the list of groups

1.1.3.3 Modify a Group

Modify a Group depicts the events for allowing the Admin Role to modify a group in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.





1.1.3.4 Modify a Group Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

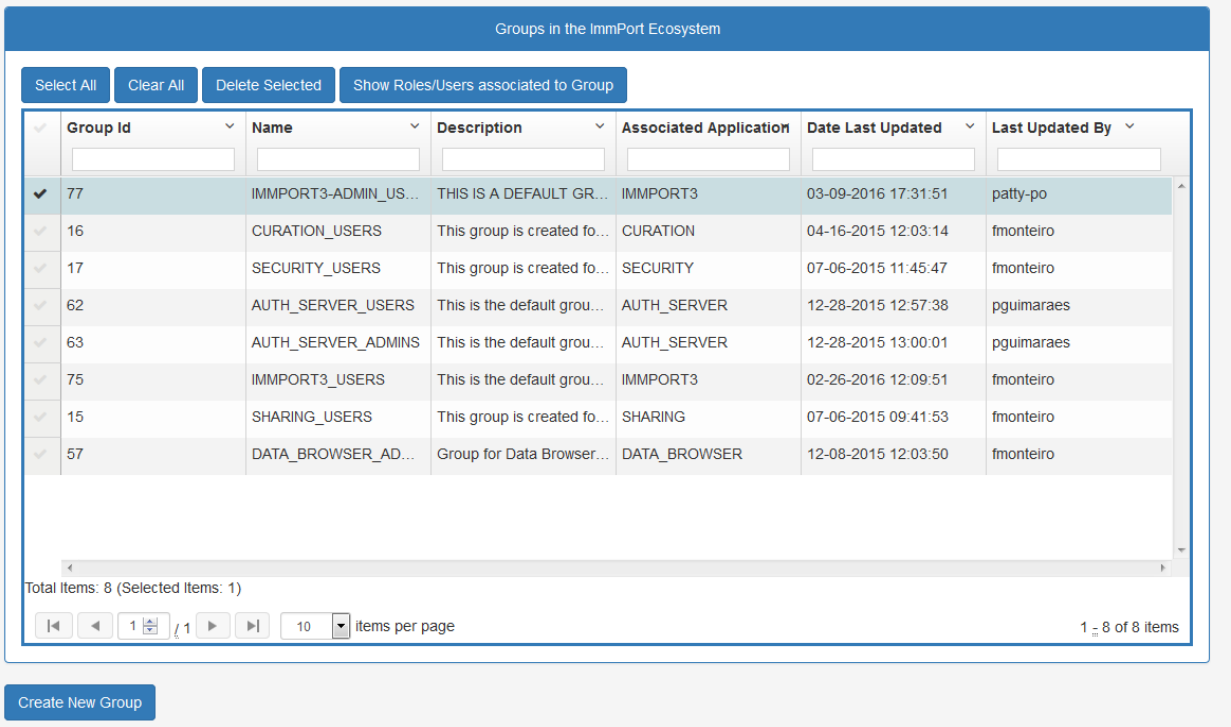
Post- Conditions: A group will be modified in the ImmPort3 Ecosystem

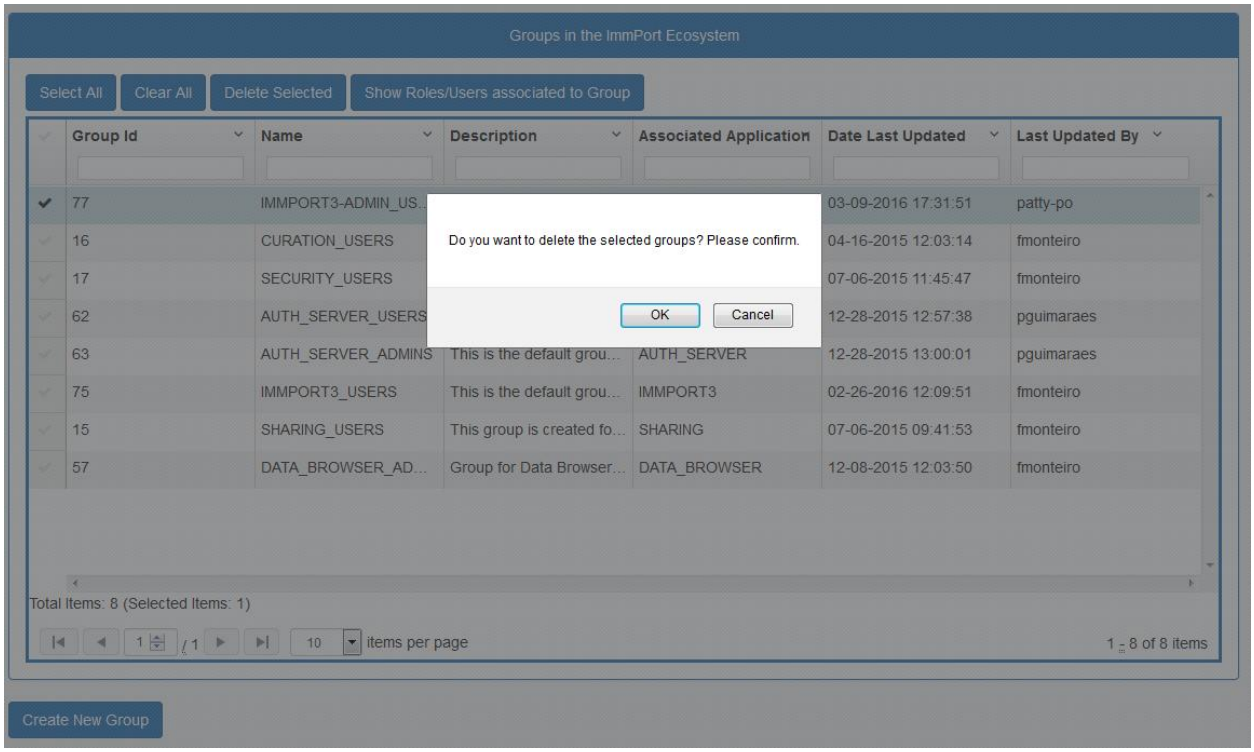
Steps:

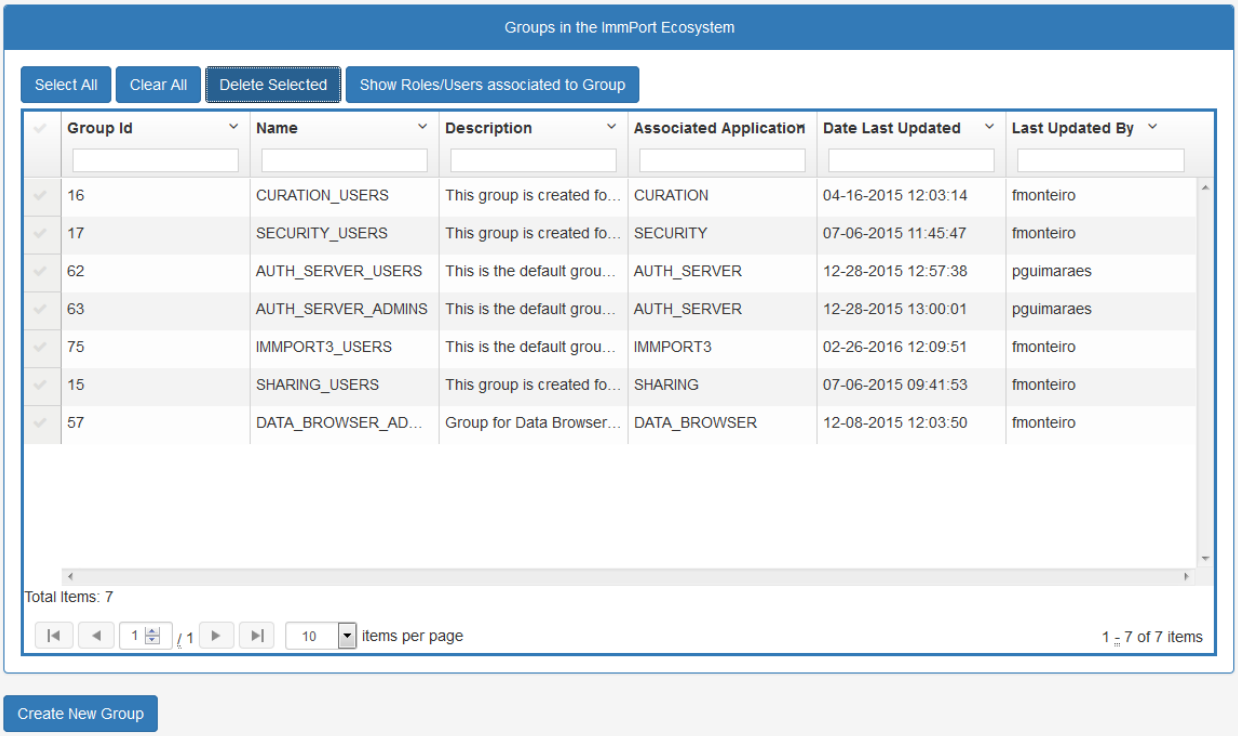
1. The admin double clicks a group name or group description.
2. The admin modifies the name or description in place.
3. The name and description is changed once the mouse looses focus on the cell.
4. The date last updated and last updated by is modified.

1.1.3.5 Delete a Group

Delete a Group depicts the events for allowing the Admin Role to delete a group in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.







1.1.3.6 Delete a Group Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

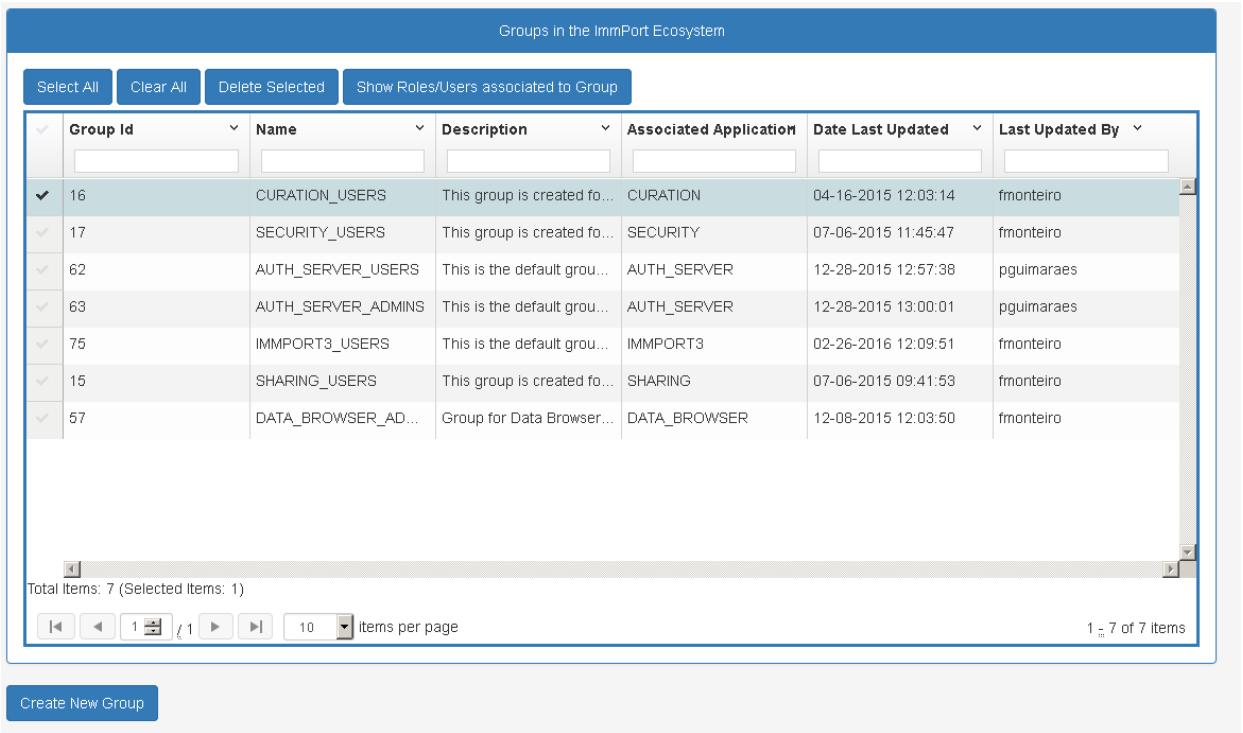
Post- Conditions: A group will be deleted in the ImmPort3 Ecosystem

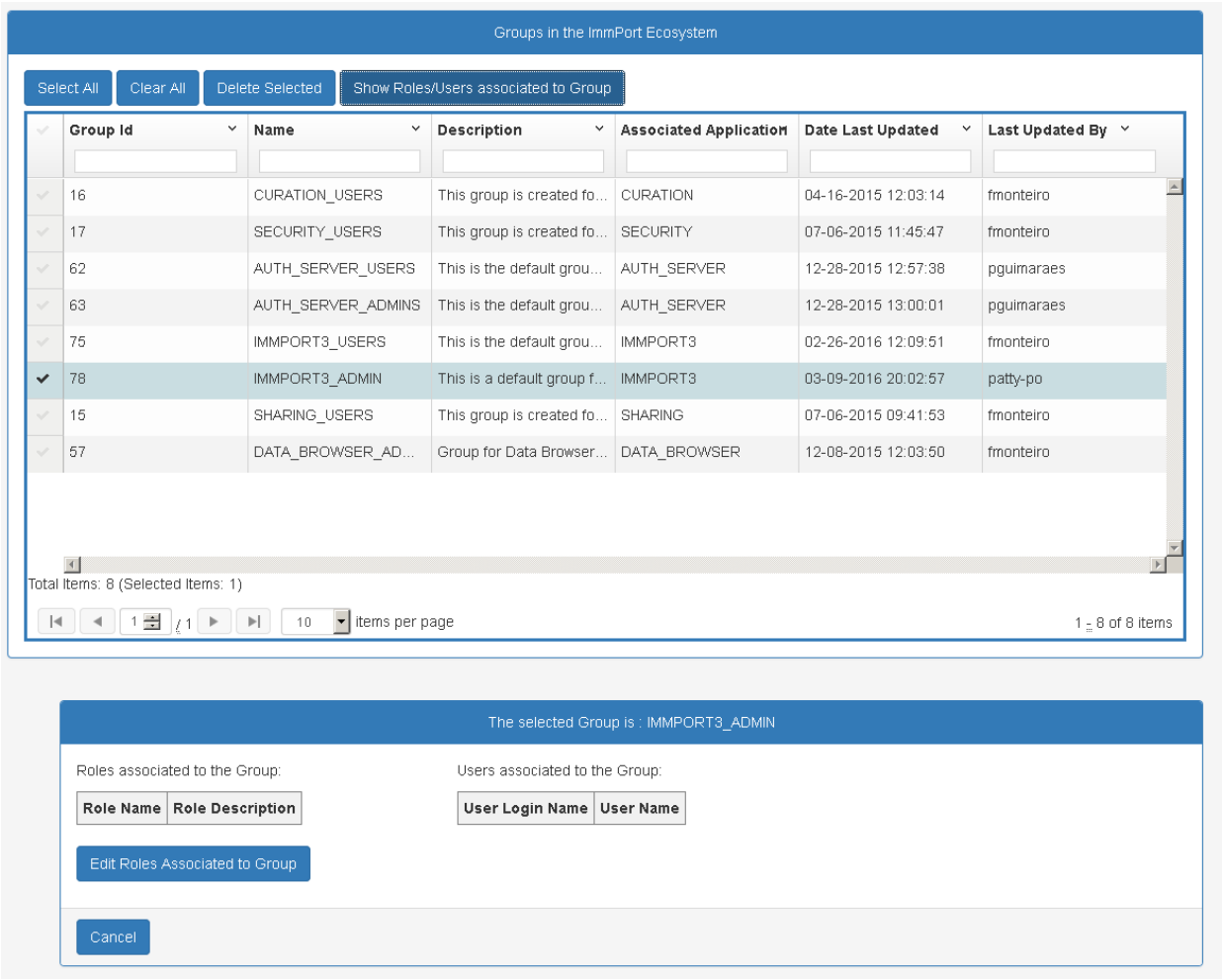
Steps:

1. The admin selects a Group.
2. The admin clicks on Deleted Selected.
3. If the group is not associated to Users, the group is deleted.
4. If it is associated, a message is displayed indicating the same.

1.1.3.7 Show Roles and User associated to the Group

Show Roles and User associated to the Group depicts the events for allowing the Admin Role to view the roles and user associated to the group in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.





1.1.3.8 Show Roles and User associated to the Group Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

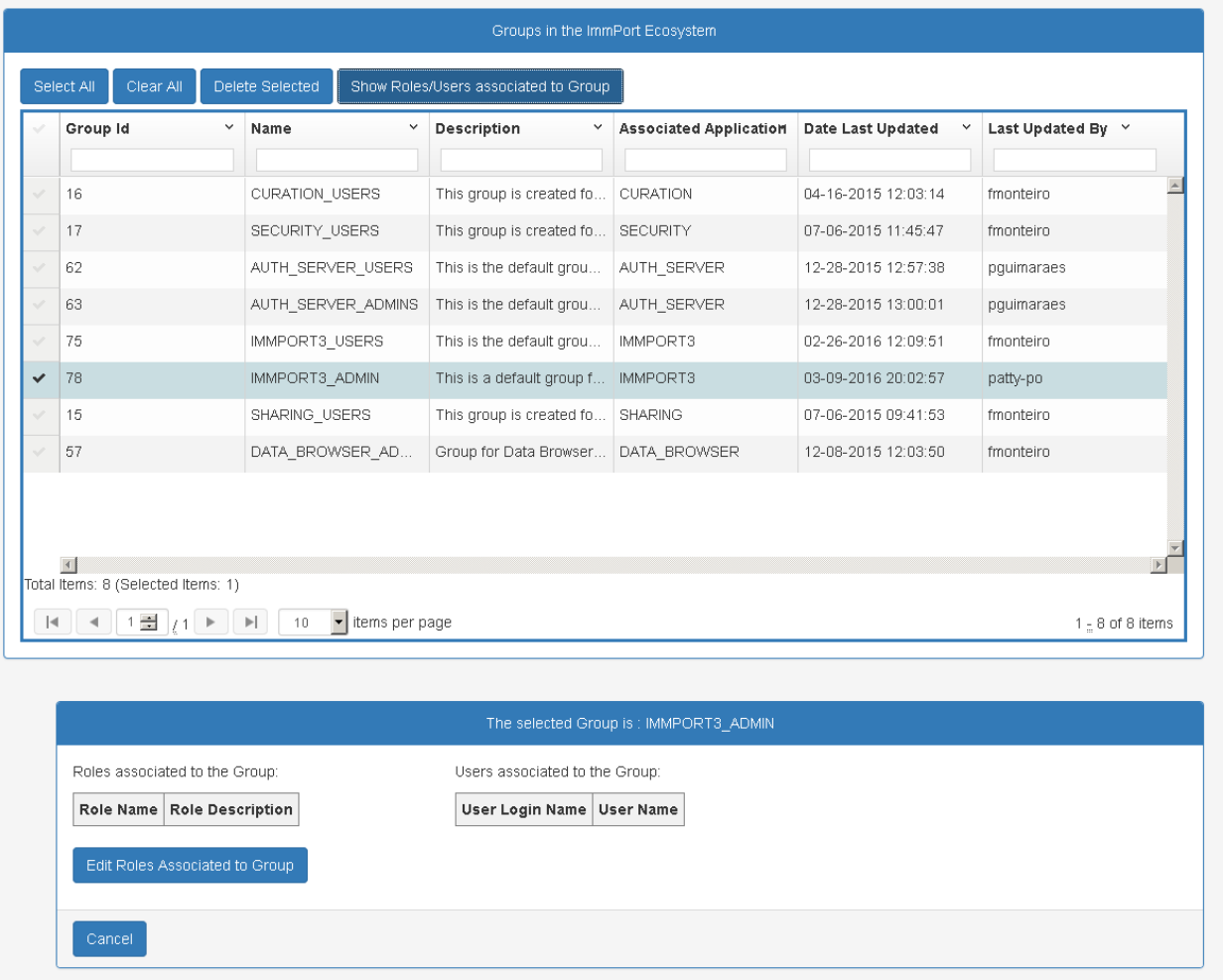
Post- Conditions: An Admin is able to view the roles and user association to a group.

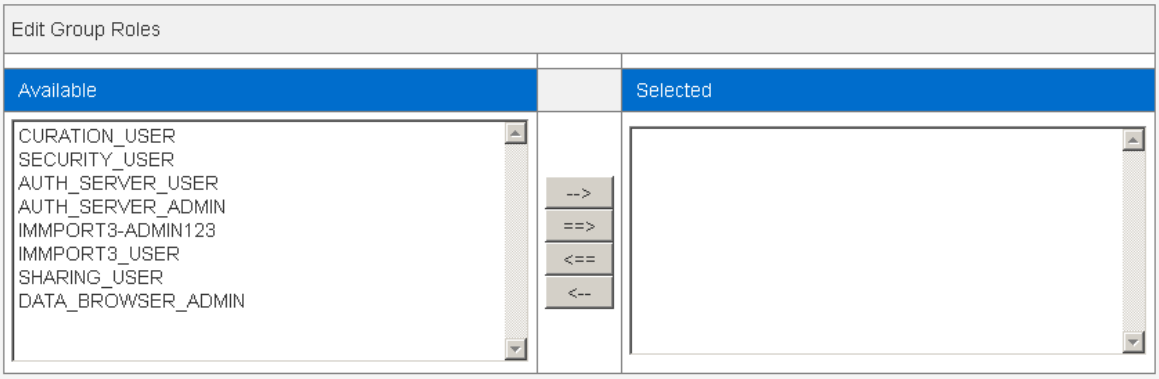
Steps:

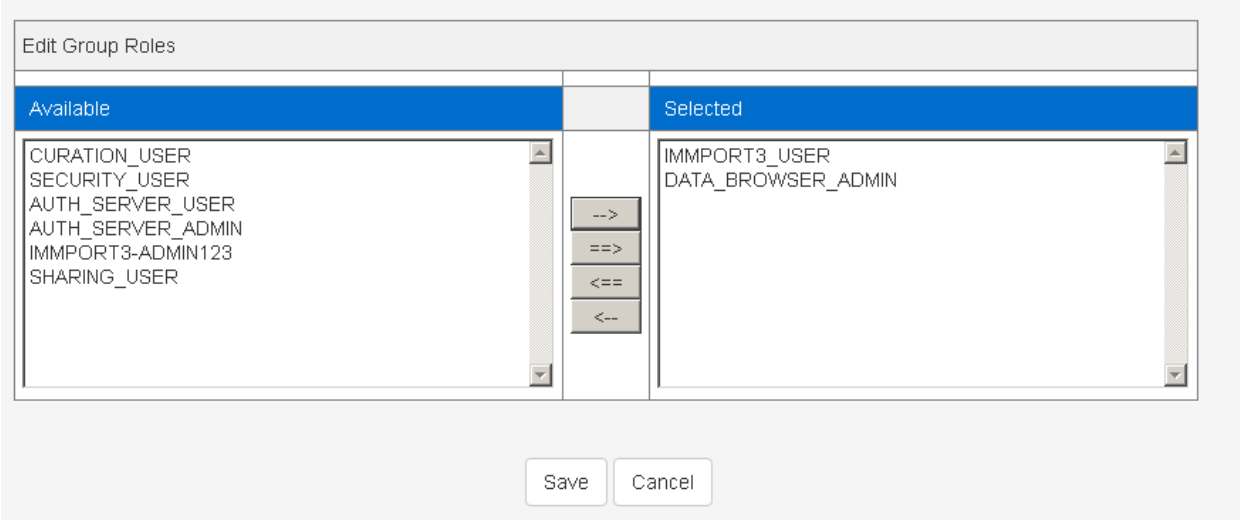
1. The admin selects a group from the list.
2. The admin clicks on the Show Roles/Users associated to the Group.
3. The system display the roles and users associated to the Group.

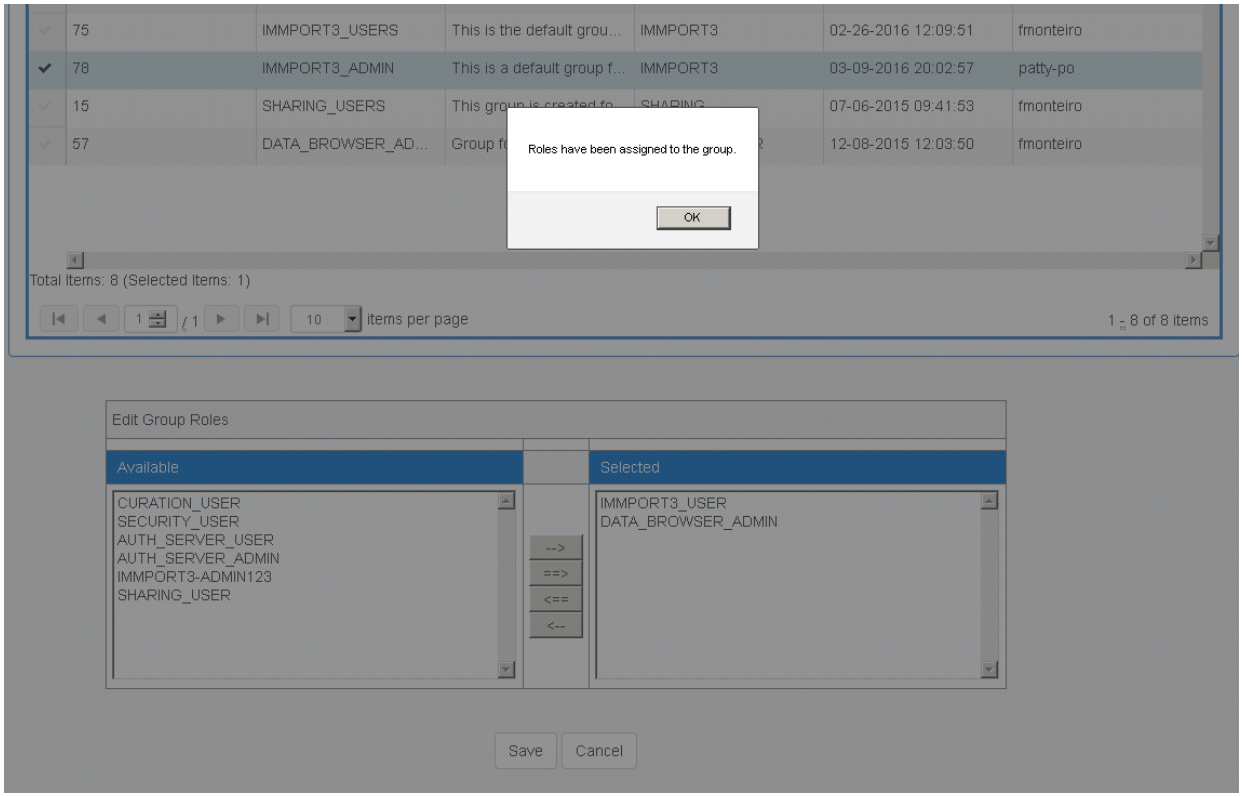
1.1.3.9 Edit Roles associated to the Group

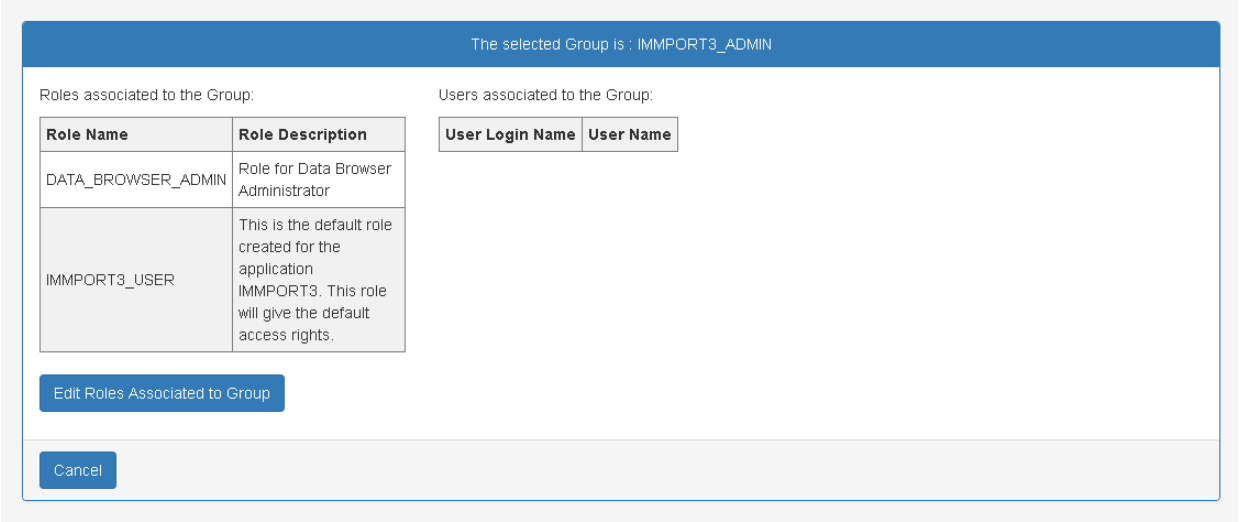
Edit Roles associated to the Group depicts the events for allowing the Admin Role to edit the roles and user associated to the group in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.






Edit Group Roles
Available
Selected
CURATION_USER
SECURITY_USER
AUTH_SERVER_USER
AUTH_SERVER_ADMIN
IMMPORT3-ADMIN123
SHARING_USER
IMMPORT3_USER
DATA_BROWSER_ADMIN
-->
==>
<==
<--
Save
Cancel


75 IMMPORT3_USERS This is the default grou... IMMPORT3 02-26-2016 12:09:51 fmonteiro
78 IMMPORT3_ADMIN This is a default group f... IMMPORT3 03-09-2016 20:02:57 patty-po
15 SHARING_USERS 07-06-2015 09:41:53 fmonteiro
57 DATA_BROWSER_AD... 12-08-2015 12:03:50 fmonteiro
Roles have been assigned to the group.
OK
Total Items: 8 (Selected Items: 1)
items per page
1 - 8 of 8 items
Edit Group Roles
Available
Selected
CURATION_USER
SECURITY_USER
AUTH_SERVER_USER
AUTH_SERVER_ADMIN
IMMPORT3-ADMIN123
SHARING_USER
IMMPORT3_USER
DATA_BROWSER_ADMIN
Save
Cancel



1.1.3.10 Edit Roles associated to the Group Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

Post- Conditions: An Admin is able to edit the roles and user association to a group.

Steps:

1. The admin selects a group from the list.
2. The admin clicks on the Show Roles/Users associated to the Group.
3. The system displays the roles and users associated to the Group.
4. The admin clicks on the Edit Roles Associated to the Group button.
5. Please refer to the screens on how to modify the roles associated to a Group.

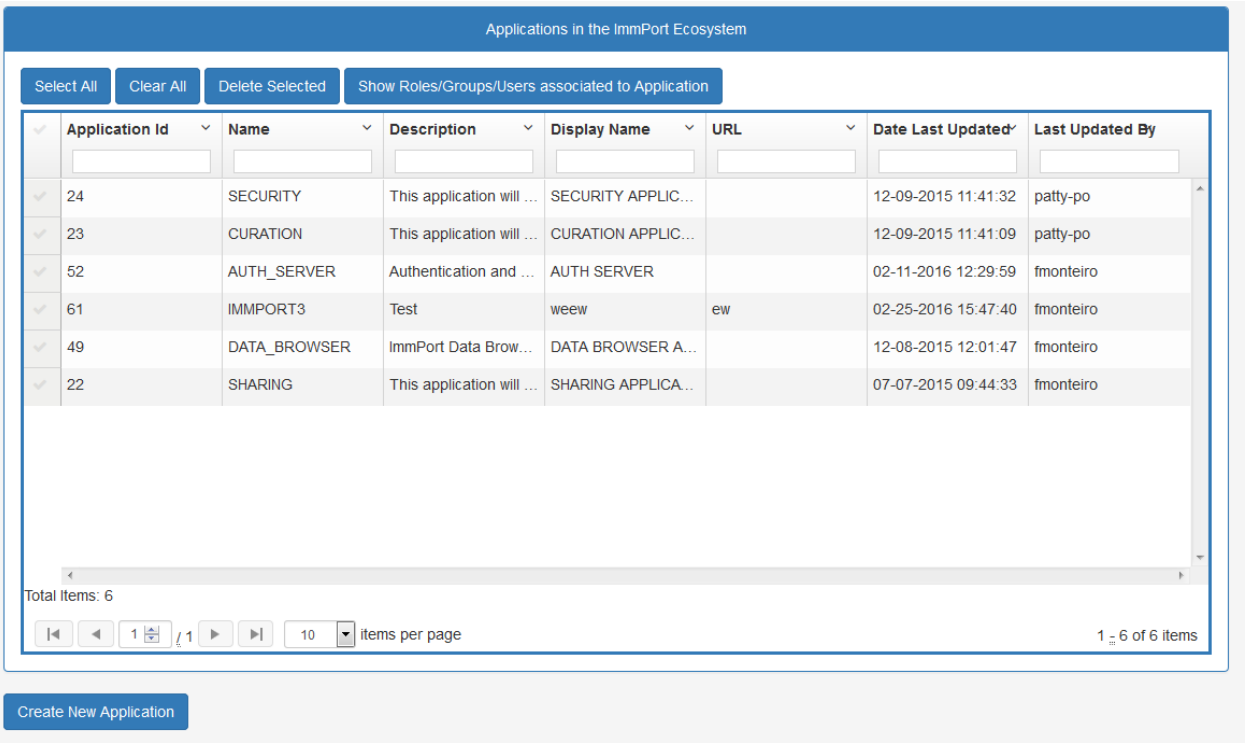
Business Rules

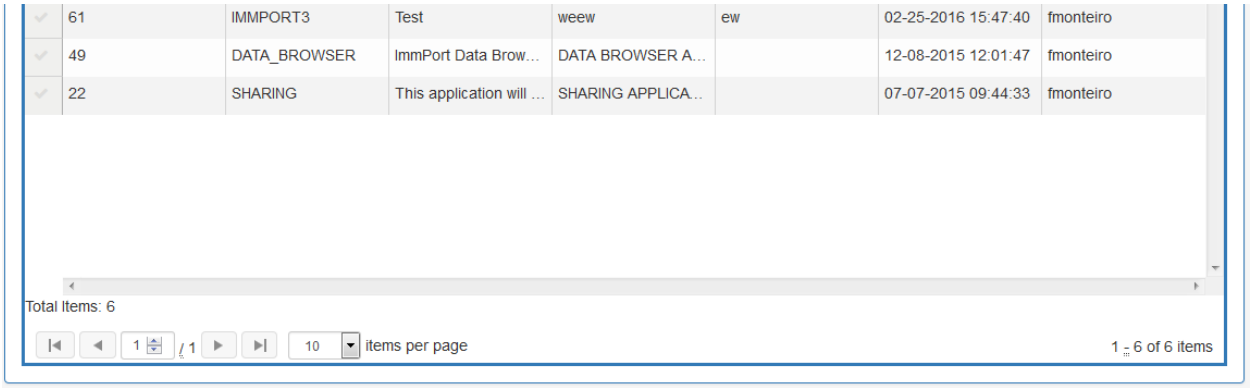
- A Group is assigned to a Particular Application.
- Every user by default will be assigned a role USER. This role will give the user basic access to the ImmPort Ecosystem.
- The different applications that belong to the ImmPort Ecosystem will be configured in the APPLICATION_INFO table. For example: The Sharing Application may have it's name configured as SHARING in the APPLICATION_INFO table.
- Groups will be configured by Applications. The group name will have the naming convention as {APPLICATION_NAME}_{GROUPNAME}. For example the SHARING application can have groups like SHARING_USER, SHARING_ADMINS, etc.
- The groups will be assigned roles. The role name will have the naming convention as {APPLICATION_NAME}_{ROLENAME}. For example the SHARING application can have groups like SHARING_USER, SHARING_ADMIN, etc.

- The groups will also be assigned to a user.
- The roles for a user will be retrieved via groups.

1.1.3.11 Add an Application

Add an Application depicts the events for allowing the Admin Role to add an application in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.

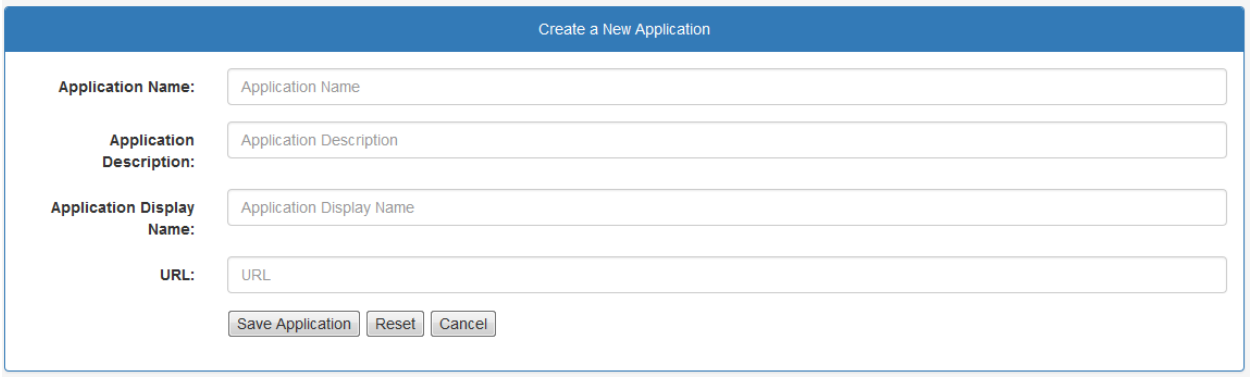




✓	61	IMMPORT3	Test	weew	ew	02-25-2016 15:47:40	fmonteiro
✓	49	DATA_BROWSER	ImmPort Data Brow…	DATA BROWSER A…		12-08-2015 12:01:47	fmonteiro
✓	22	SHARING	This application will …	SHARING APPLICA…		07-07-2015 09:44:33	fmonteiro

Total Items: 6

1 / 1 10 items per page 1 - 6 of 6 items



Create a New Application

Application Name: Application Name

Application Description: Application Description

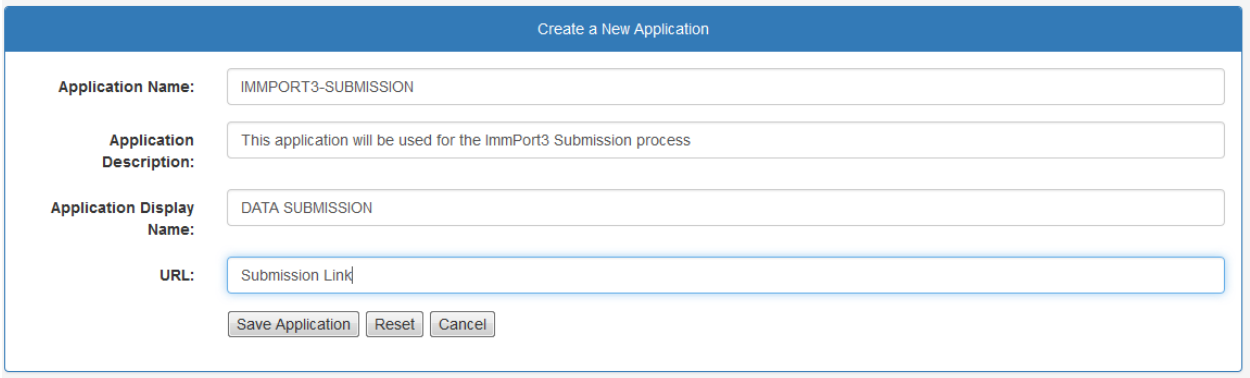
Application Display Name: Application Display Name

URL: URL

Save Application | Reset | Cancel

Total Items: 6

1 / 1 10 items per page 1 - 6 of 6 items



Create a New Application

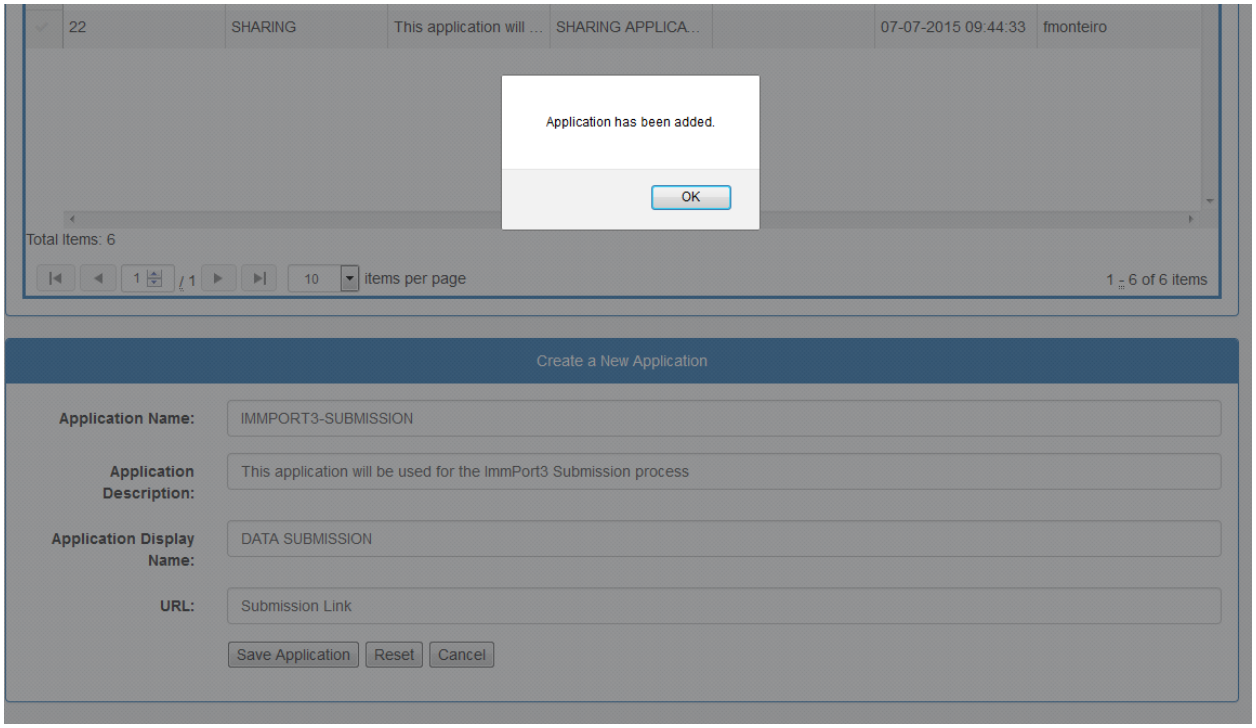
Application Name: IMMPORT3-SUBMISSION

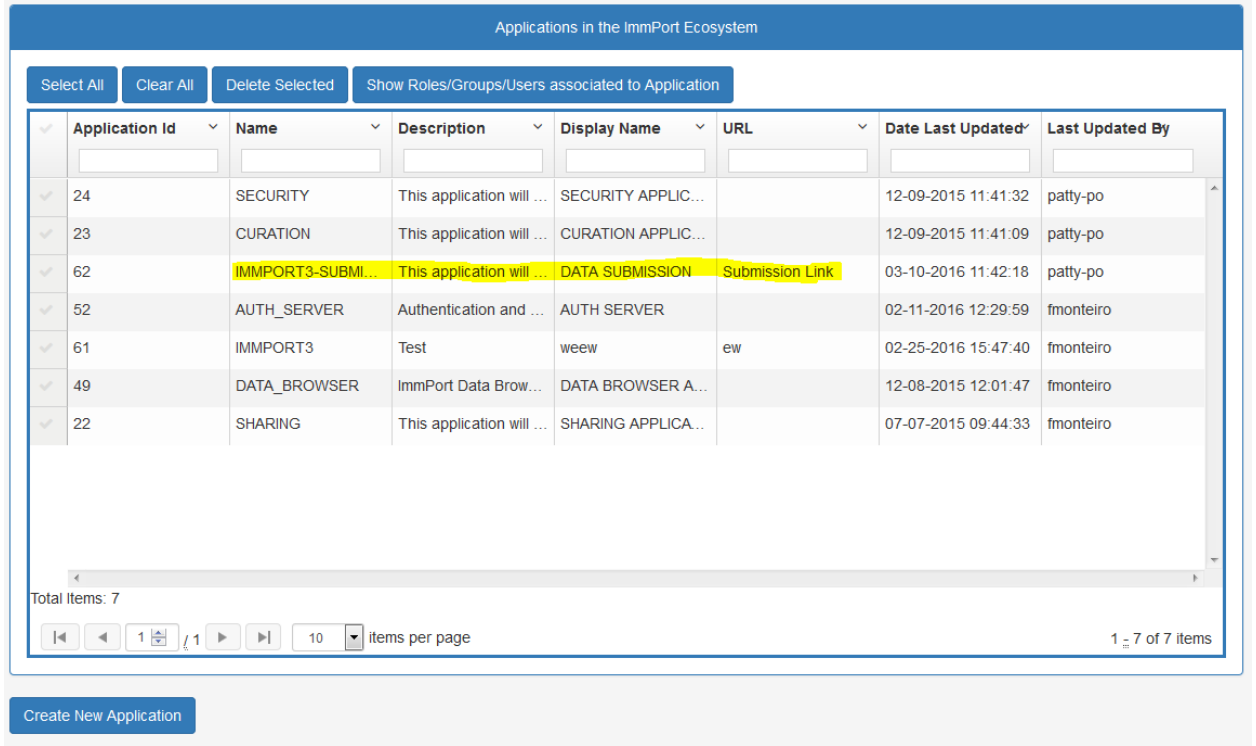
Application Description: This application will be used for the ImmPort3 Submission process

Application Display Name: DATA SUBMISSION

URL: Submission Link

Save Application | Reset | Cancel





1.1.3.12 Add an Application Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

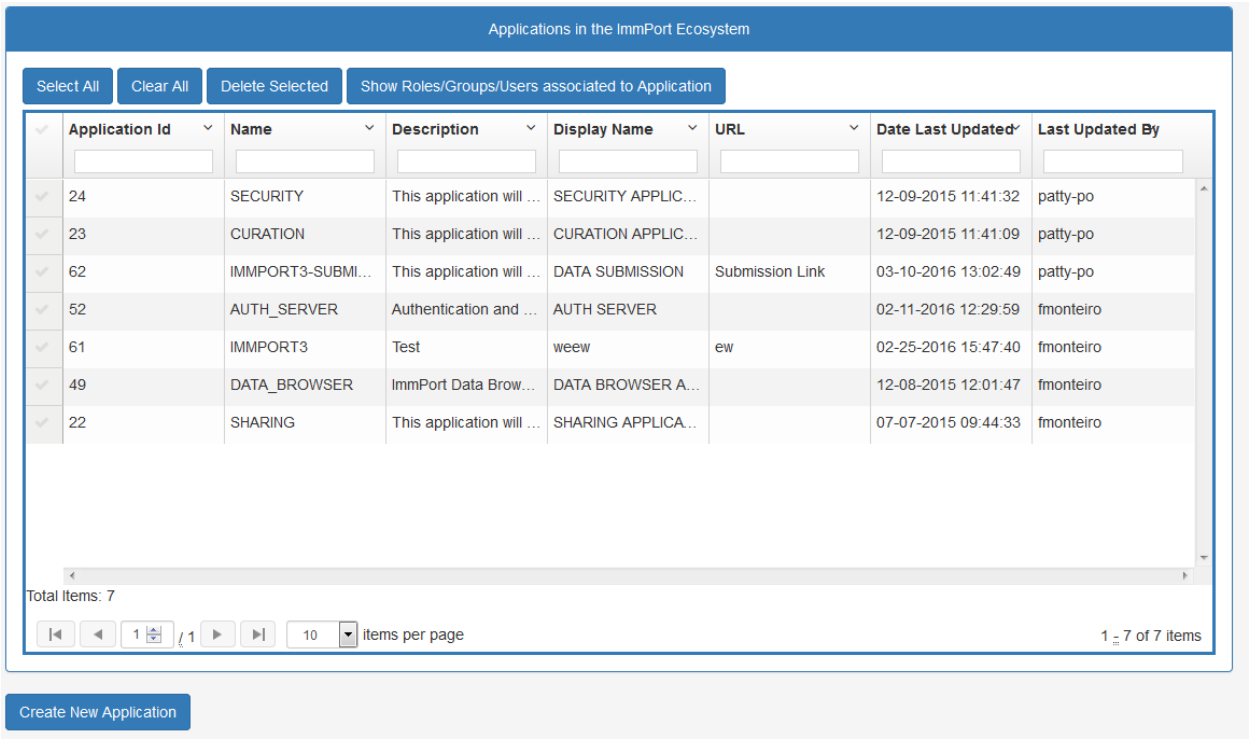
Post- Conditions: An application will be created.

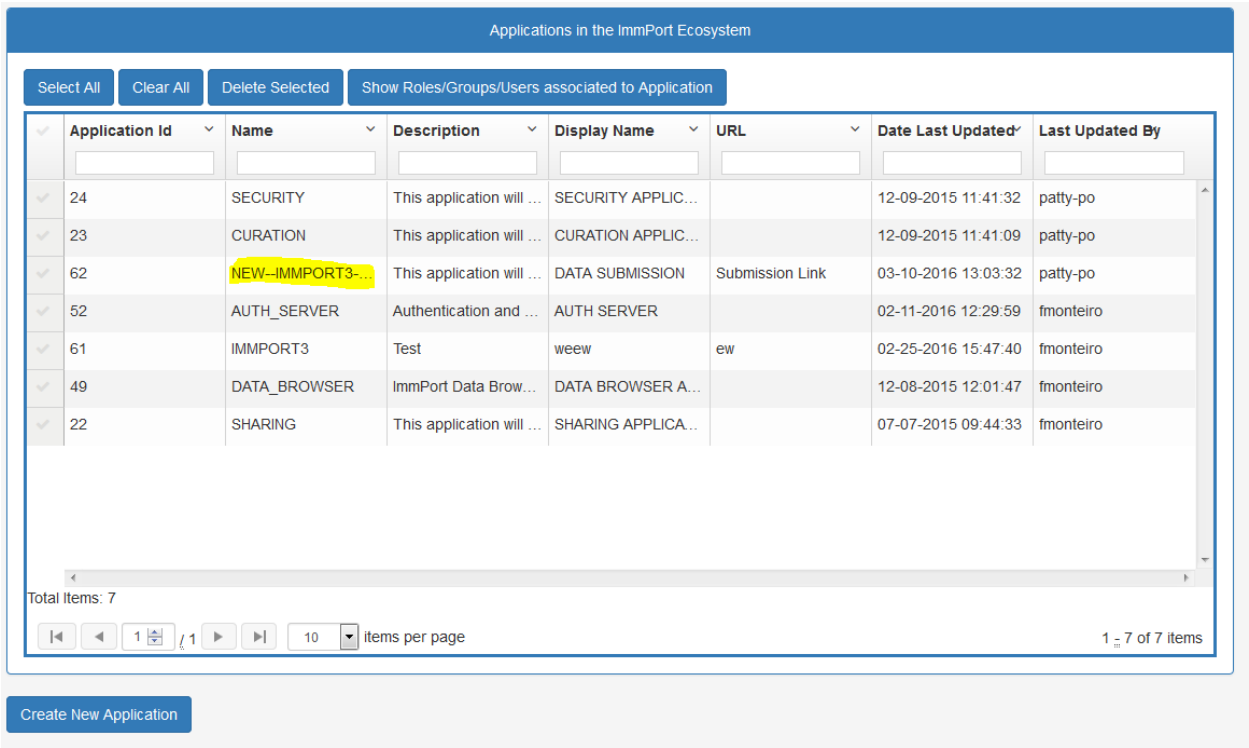
Steps:

1. The admin clicks on the Create New Application button.
2. The admin enters the application name, description, display name and URL.
3. The admin clicks Save Application.
4. The system saves the application in the database and it is displayed in the list of applications.

1.1.3.13 Modify an Application

Modify an Application depicts the events for allowing the Admin Role to modify an application in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.





1.1.3.14 Modify an Application Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

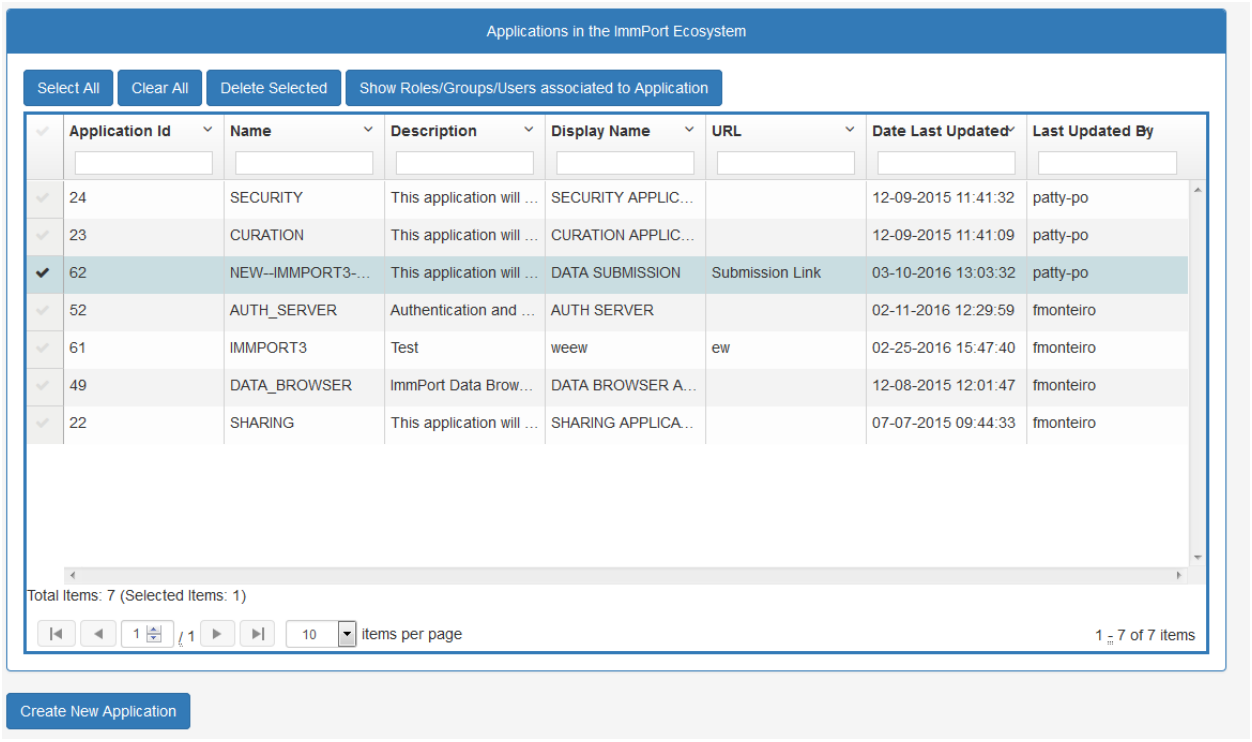
Post- Conditions: An application will be modified by the admin user.

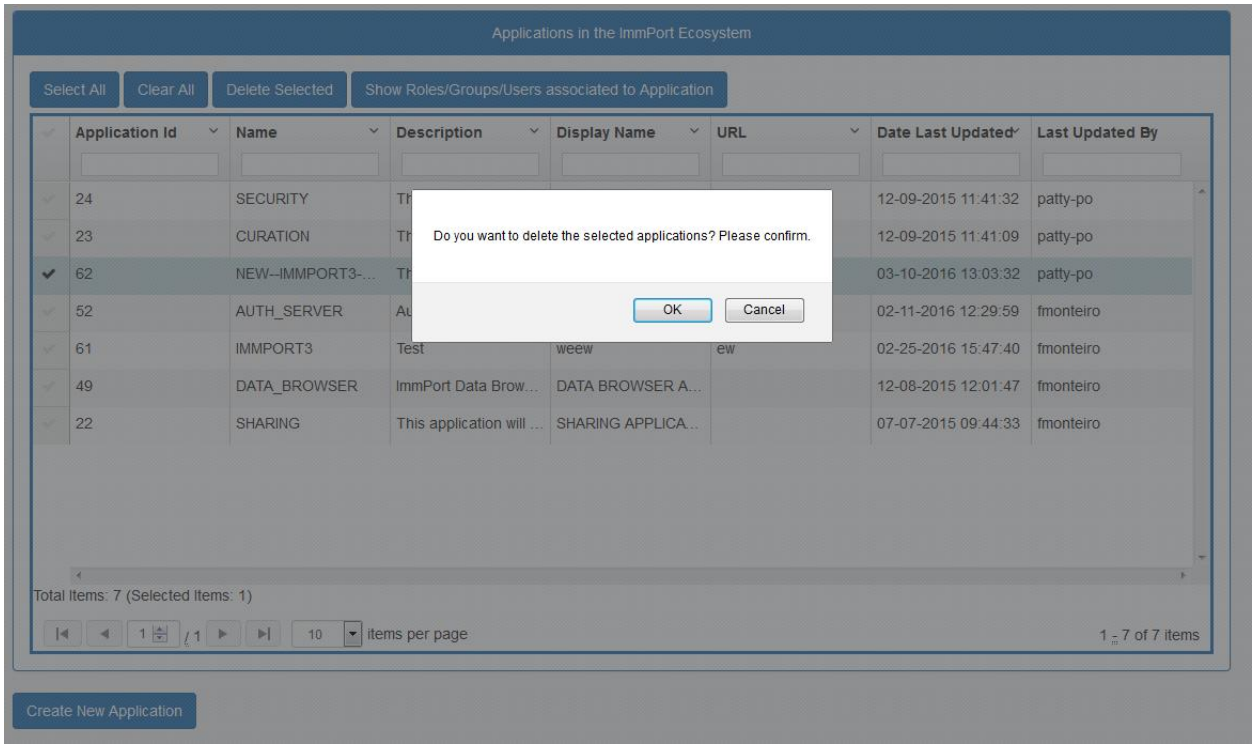
Steps:

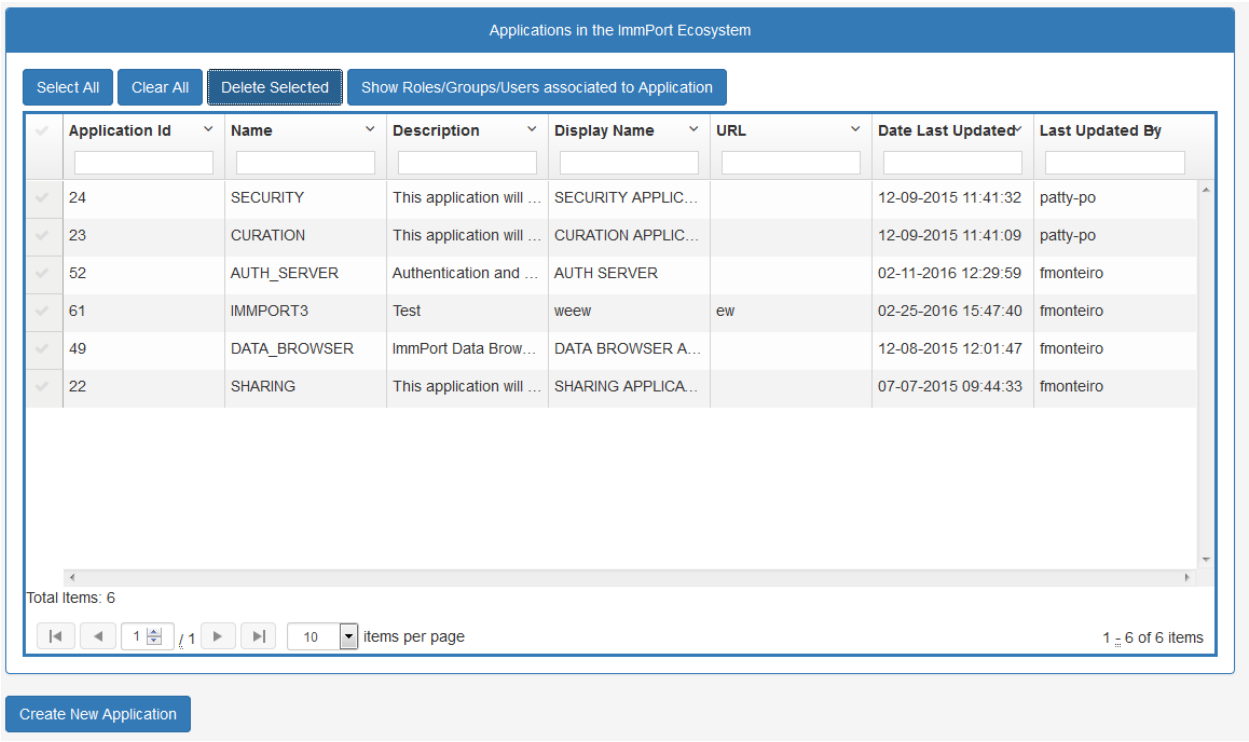
1. The admin double clicks an application name or application description.
2. The admin modifies the name or description or display name or URL in place.
3. The name and description is changed once the mouse looses focus on the cell.
4. The date last updated and last updated by is modified.

1.1.3.15 Delete an Application

Delete an Application depicts the events for allowing the Admin Role to delete an application in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.


Applications in the ImmPort Ecosystem
Select All
Clear All
Delete Selected
Show Roles/Groups/Users associated to Application
Application Id
Name
Description
Display Name
URL
Date Last Updated
Last Updated By
24 SECURITY This application will ... SECURITY APPLIC... 12-09-2015 11:41:32 patty-po
23 CURATION This application will ... CURATION APPLIC... 12-09-2015 11:41:09 patty-po
62 NEW--IMMPORT3-... This application will ... DATA SUBMISSION Submission Link 03-10-2016 13:03:32 patty-po
52 AUTH_SERVER Authentication and ... AUTH SERVER 02-11-2016 12:29:59 fmonteiro
61 IMMPORT3 Test weew ew 02-25-2016 15:47:40 fmonteiro
49 DATA_BROWSER ImmPort Data Brow... DATA BROWSER A... 12-08-2015 12:01:47 fmonteiro
22 SHARING This application will ... SHARING APPLICA... 07-07-2015 09:44:33 fmonteiro
Total Items: 7 (Selected Items: 1)
1 / 1
10 items per page
1 - 7 of 7 items
Create New Application


Applications in the ImmPort Ecosystem
Select All
Clear All
Delete Selected
Show Roles/Groups/Users associated to Application
Do you want to delete the selected applications? Please confirm.
OK
Cancel
Total Items: 7 (Selected Items: 1)
items per page
1 - 7 of 7 items
Create New Application



1.1.3.16 Delete an Application Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

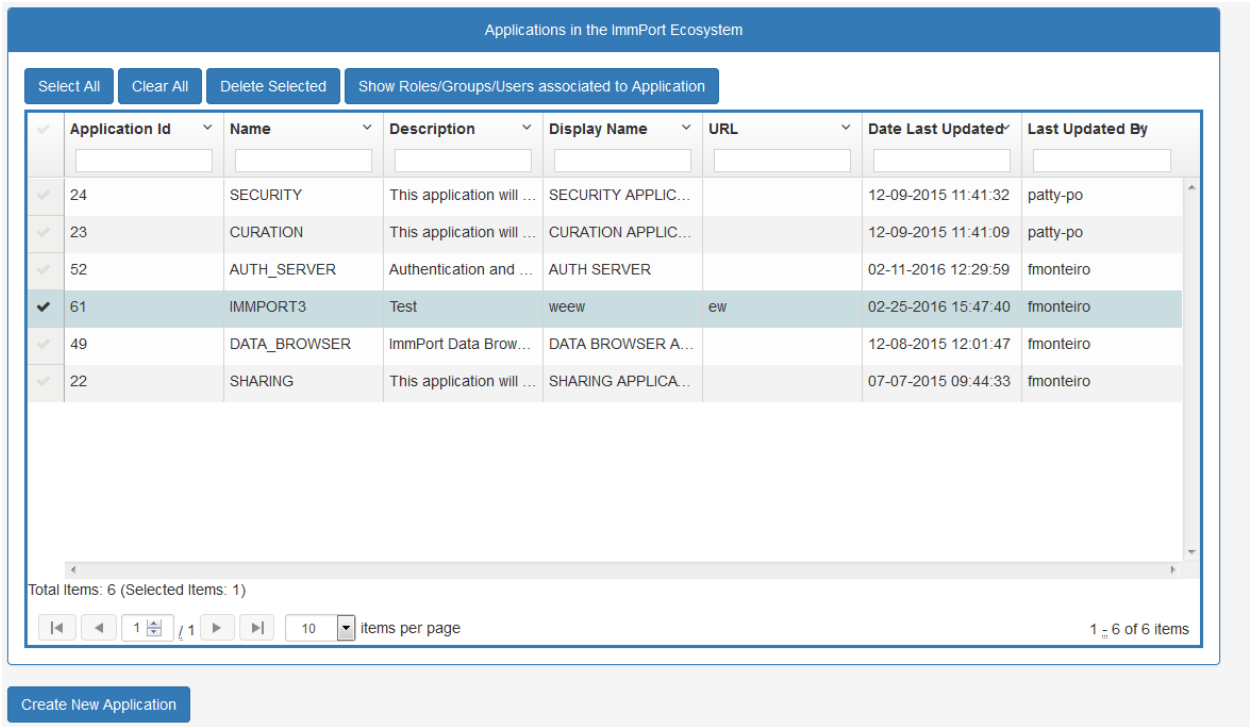
Post- Conditions: An application will be deleted by the admin user.

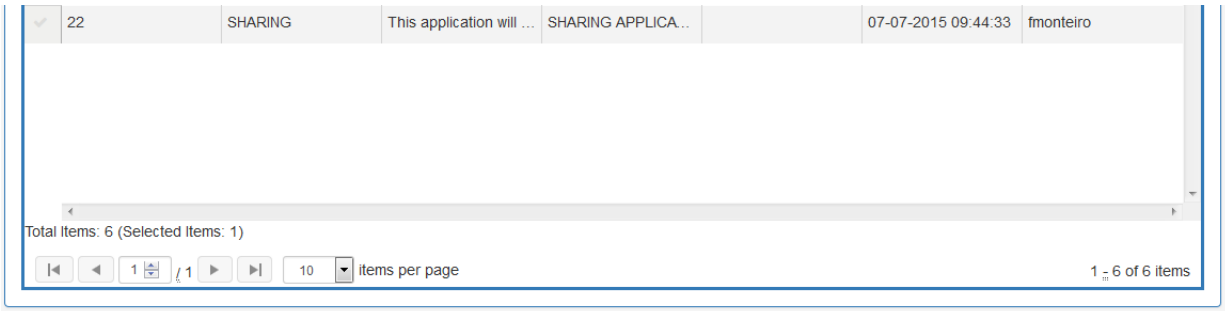
Steps:

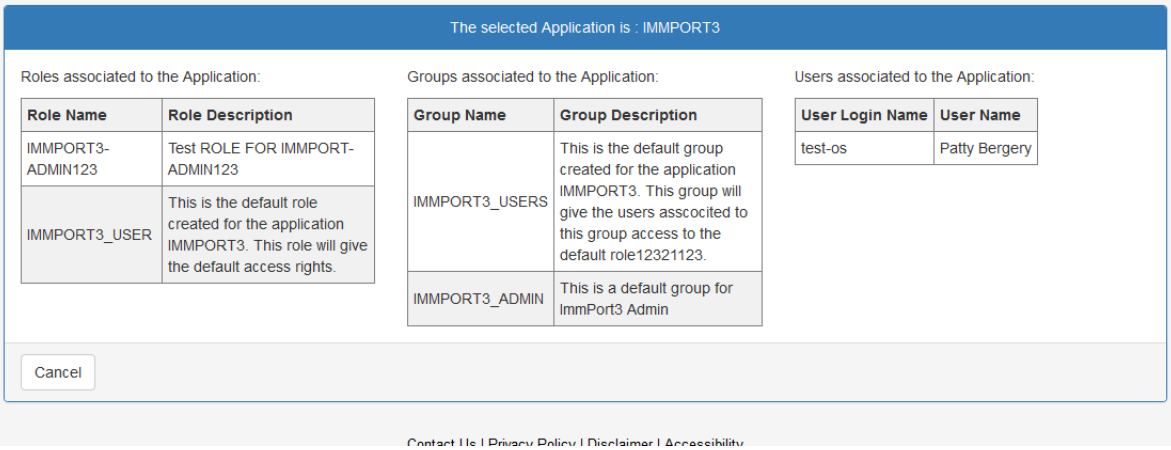
1. The admin selects an Application.
2. The admin clicks on the "Deleted Selected" button
3. If the application is not associated to Users, the application is deleted.
4. If it is associated, an error message is displayed indicating the same.

1.1.3.17 Show Roles/Groups associated to the Application

Show Roles and User associated to the Group depicts the events for allowing the Admin Role to view the roles and user associated to the group in the ImmPort3 Ecosystem. Appropriate error messages are displayed if errors are encountered.


Applications in the ImmPort Ecosystem
Select All
Clear All
Delete Selected
Show Roles/Groups/Users associated to Application
Application Id
Name
Description
Display Name
URL
Date Last Updated
Last Updated By
24 SECURITY This application will ... SECURITY APPLIC... 12-09-2015 11:41:32 patty-po
23 CURATION This application will ... CURATION APPLIC... 12-09-2015 11:41:09 patty-po
52 AUTH_SERVER Authentication and ... AUTH SERVER 02-11-2016 12:29:59 fmonteiro
61 IMMPORT3 Test weew ew 02-25-2016 15:47:40 fmonteiro
49 DATA_BROWSER ImmPort Data Brow... DATA BROWSER A... 12-08-2015 12:01:47 fmonteiro
22 SHARING This application will ... SHARING APPLICA... 07-07-2015 09:44:33 fmonteiro
Total Items: 6 (Selected Items: 1)
1 / 1
10 items per page
1 - 6 of 6 items
Create New Application


22 SHARING This application will ... SHARING APPLICA... 07-07-2015 09:44:33 fmonteiro
Total Items: 6 (Selected Items: 1)
1 / 1
10 items per page
1 - 6 of 6 items


The selected Application is : IMMPORT3
Roles associated to the Application:
Role Name
Role Description
IMMPORT3-ADMIN123
Test ROLE FOR IMMPORT-ADMIN123
IMMPORT3_USER
This is the default role created for the application IMMPORT3. This role will give the default access rights.
Groups associated to the Application:
Group Name
Group Description
IMMPORT3_USERS
This is the default group created for the application IMMPORT3. This group will give the users asscocited to this group access to the default role12321123.
IMMPORT3_ADMIN
This is a default group for ImmPort3 Admin
Users associated to the Application:
User Login Name
User Name
test-os
Patty Bergery
Cancel

1.1.3.18 Show Roles/Groups associated to the Application Use Case

Actor: A user with Admin Role.

Pre-Conditions: The user is logged into the **Security Application.**

Post- Conditions: An Admin is able to view the roles/groups associated to an application.

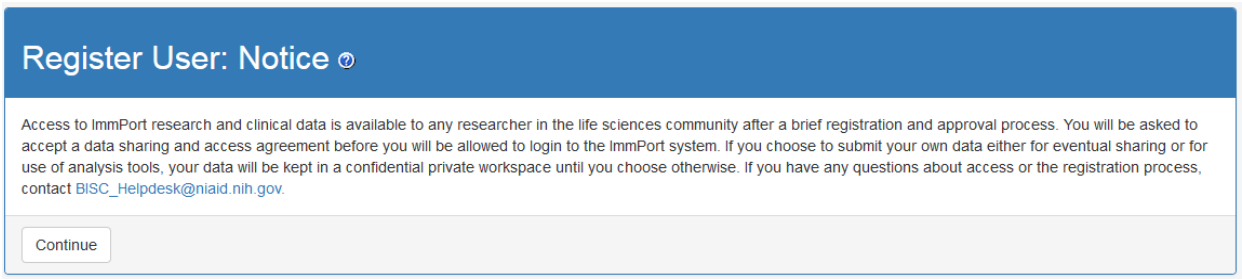
Steps:

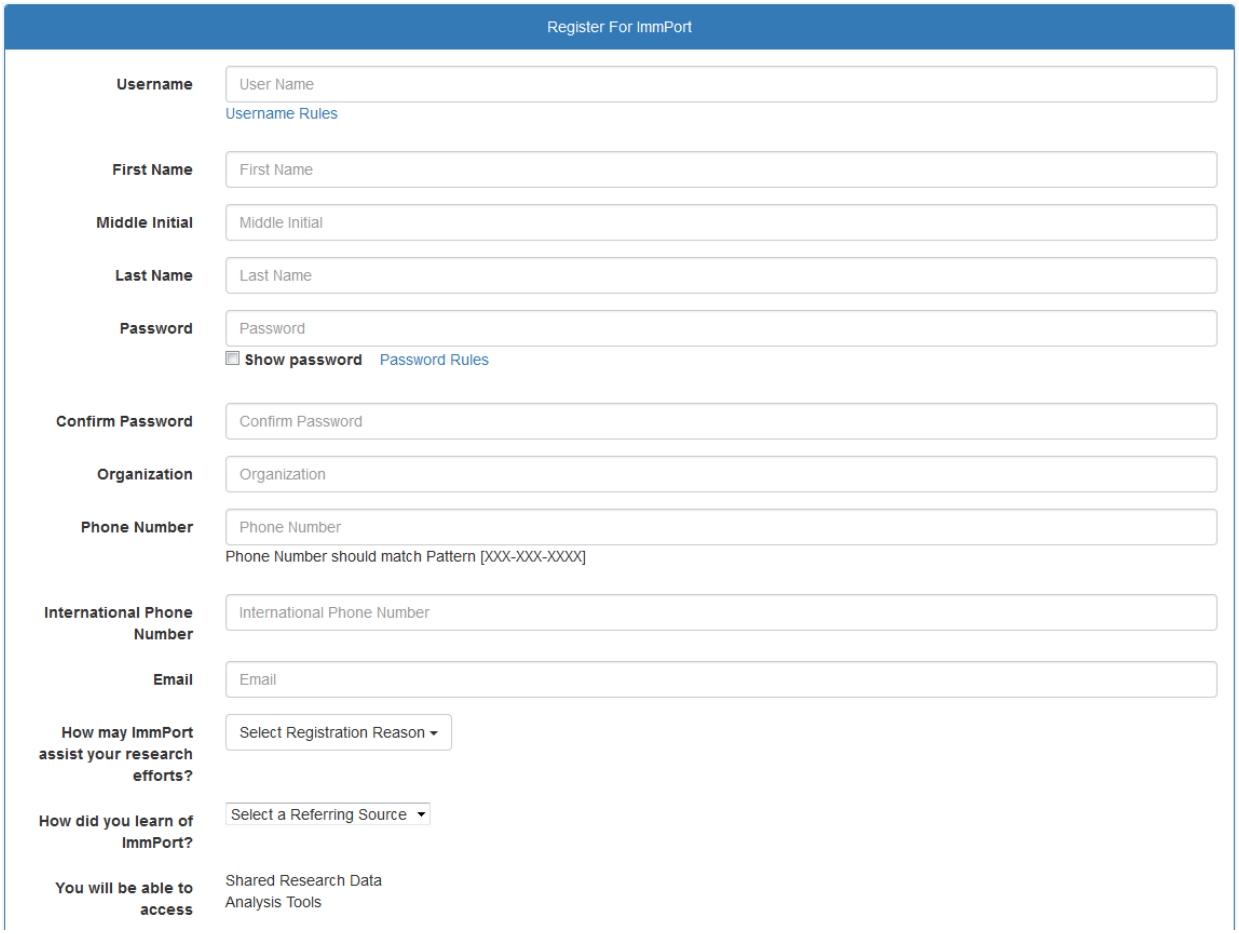
1. The admin selects an application from the list.
2. The admin clicks on the Show Roles/Groups associated to the Application.
3. The system displays the roles and groups associated to the Application.

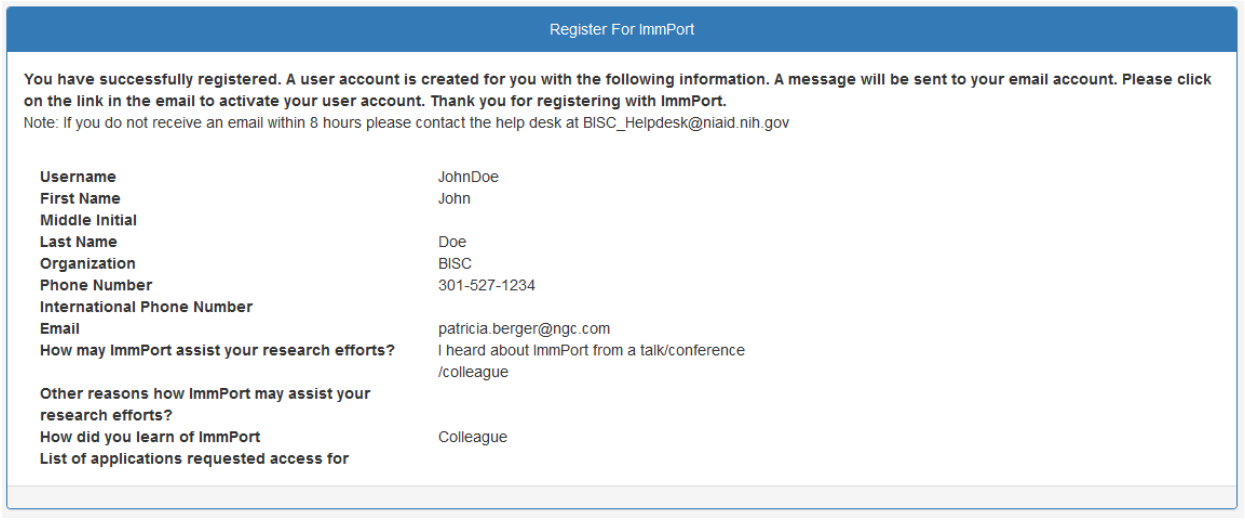
1.1.4 Manage Users

1.1.4.1 Users Registration

The User Registration depicts the events for requesting access to ImmPort. If the system encounters errors, the system will display the appropriate error message(s) to the user and state that his/her information could not be saved due to a system error and to contact the Helpdesk.







BISC_SECURITY.USER_INFO	DEVELOPER.USER_INFO	Mapping
USER_ID	USER_ID	Use the Sequence in the respective database
LAST_NAME	LAST_NAME	Maps equal

	SECRET_QUESTION_ID	Sets it to default value 1
MIDDLE_INITIAL	MIDDLE_INITIAL	Maps equal
	USER_COMMUNITY_ID	Set to default value LS
FIRST_NAME	FIRST_NAME	Maps equal
EMAIL_ADDRESS	EMAIL_ADDRESS	Maps equal
PASSWORD	PASSWORD	Maps equal
	SECRET_QUESTION_ANSWER	Set to default value 'Dummy Answer'
DATE_CREATED	DATE_CREATED	Set to value = sysdate
DATE_LAST_UPDATED	DATE_LAST_UPDATED	Set to value = sysdate
ORGANIZATION	ORGANIZATION	Maps equal
LAST_UPDATED_BY	LAST_UPDATED_BY	Set to value 'registeruser'
USERNAME	USER_LOGIN_NAME	Maps equal
	ADDRESS	Set to NULL
RESET_PASSWORD_FLAG	RESET_PASSWORD_FLAG	Set to N
	EMPLOYEE_ID	Set to NULL
	APPROVED_BY	Set to NULL
	CREATED_BY	Set to value 'registeruser'
	AGREEMENT_DATE	Set to NULL
	AGREEMENT_ACCEPTANCE	Set to NULL
	DEPARTMENT	Set to NULL
	PI_NAME	Set to NULL
	INTL_PHONE_NUMBER_FLAG	When BISC_USER_INFO PHONE_NUMBER IS NULL OR EMPTY THEN 'Y' ELSE 'N' END
	PHONE_NUMBER	if BISC_USER_INFO.PHONE_NUMBERIS NULLAND BISC_USER_INFO.INTL_PHONE_NUMBER IS NOT NULL THEN BISC_USER_INFO.INTL_PHONE_NUMBER else if BISC_USER_INFO.INTL_PHONE_NUMBER IS NULL

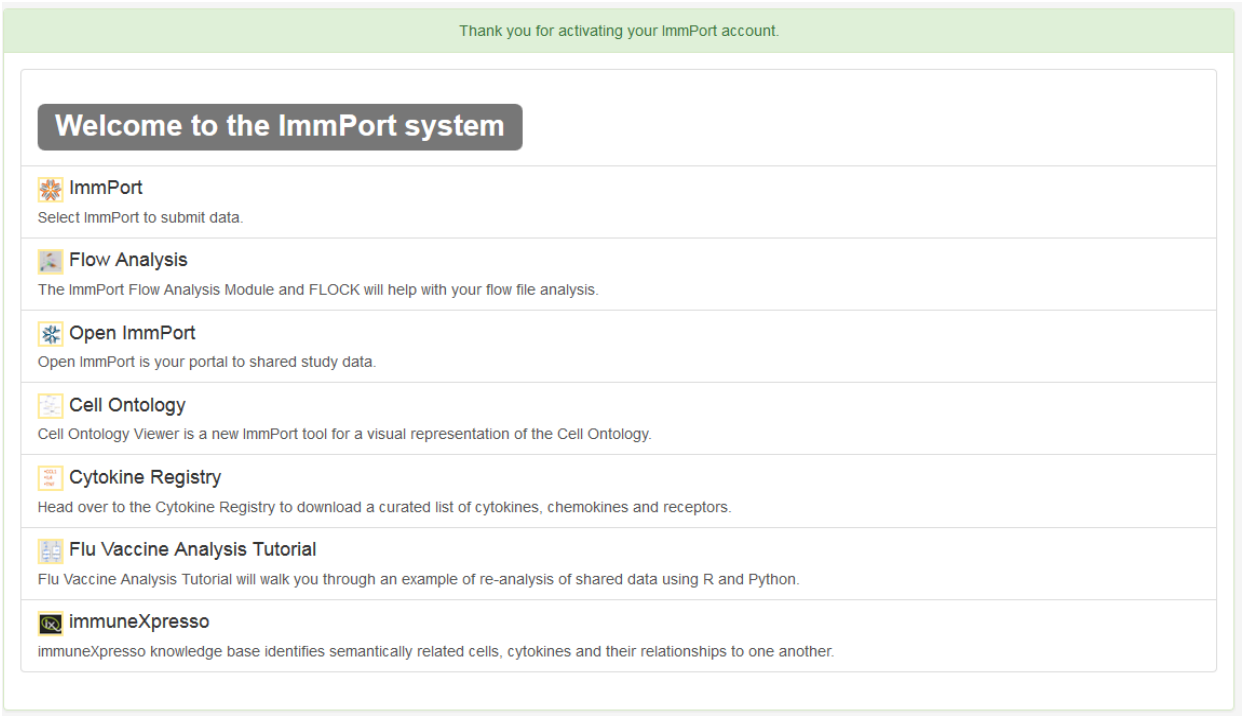
		AND BISC_USER_INFO.PHONE _NUMBER IS NOT NULL THEN BISC_USER_INFO.PHONE _NUMBER ELSE '000-000-0000
USER_STATUS	USER_STATUS_ID	CASE WHEN BISC_USER_INFO.USER_ STATUS = 'Pending' THEN 'P' WHEN BISC_USER_INFO.USER_ STATUS = 'Active' THEN 'A' WHEN BISC_USER_INFO.USER_ STATUS = 'Rejected' THEN 'R' WHEN BISC_USER_INFO.USER_ STATUS = 'Inactive' THEN 'I' ELSE NULL END
REGISTER_REASONS	WHY_REGISTER	Maps equal
REFERRING_SOURCE	REFERENCE_ID	CASE WHEN :new.REFERRING_SOURC E = 'Colleague' THEN 1 WHEN :new.REFERRING_SOURC E = 'DAIT_Staff' THEN 2 WHEN :new.REFERRING_SOURC E = 'Other' THEN 9 ELSE NULL END

Subject: EXT :Registration Confirmation

Dear John Doe,

Thank you for registering with ImmPort. An account was created for you. Please click on the link below to activate your account.
Click here to confirm your registration

This is an automated message. Please do not reply to this email, but contact BISC_HELPDESK@mail.nih.gov if you have any questions.



1.1.4.2 Users Registration Use Case

The User Registration describes the process for registering for a user account.

Actor: Any user without an account.

Pre-Conditions: The user is new to the system and registering for the first time

Post- Conditions: A user is created in the system with the default User Role.

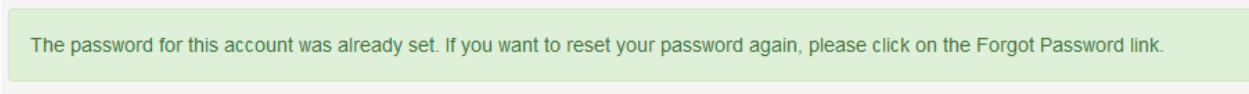
Steps:

1. The user clicks on the Sign up Free or Register for ImmPort Link on the ImmPort Production site.
2. The system will direct the user to the Security Application.
3. A "**Register User: Notice**" screen is displayed, the user clicks on the Continue button.
4. The system will display the "**Register User**" screen.
5. The user enters profile data.
6. The user clicks on the Register button.
7. The system stores the created user account in Pending Status in the database.

8. The system creates a user in the ImmPort 2 database. There is a trigger on the BISC_SECURITY.USER_INFO to populate the table in the DEVELOPER.USER_INFO schema. Please refer to the trigger TR_AIU_BISC_USER_INFO.
9. A unique verification code is created for the user and the status is set to "User token has been sent to the user and is pending verification".
10. An email is created with a link which contains the verification token and is sent to the email address registered on the account.
11. The system displays a message indicating that the user has been sent a mail with a link and he will need to click the link to confirm his registration and summary of his profile as shown in User Profile Summary screen.
12. The user receives a confirmation email with a link as shown in the Email Confirmation screenshot.
13. The user clicks on the link and the system activates the account and Pending status is changed to Active Status.
14. The system sets the verification code to the status "User is verified".
15. The user is displayed the Account Activation screen.
16. The user can then login to the original application with his username and password.

1.1.4.3 Email Activation Link

The system will display a message when a user clicks the reset password link when it has already been clicked.



1.1.4.4 Email Activation Link Use Case (Used Link)

The Email Activation describes the process for a user to activate their account when they have already clicked the link to activate the account.

Actor: A user with an account.

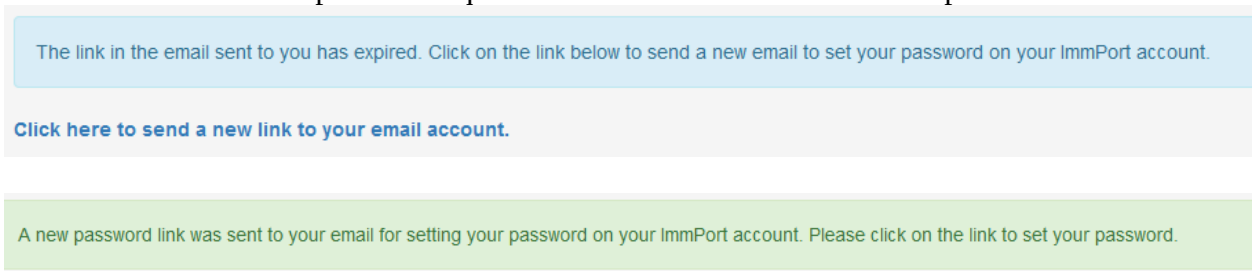
Pre-Conditions: The user already activated their account.

Post- Conditions: A message is displayed to instruct the user to click on the “Forgot Password” link.

1. The user clicks on the email link again.
2. The system display the message that user is already activated.
3. The system displays the Account Already Activated Page.

1.1.4.5 Email Activation Link Expired

The Email Activation depicts the sequence when an activation link has expired.



1.1.4.6 Email Activation Link Use Case (Expired Link)

The Email Activation Link describes the process for registering a user account when the link expired.

Actor: A user with an account.

Pre-Conditions: The email link to activate the user's account has expired.

Post- Conditions: A message is displayed to instruct the user to click on the new link.

1. The user clicks on the email link after the configurable expiration period.
2. The system displays the Email Activation Link Expired page which shows a message that the link has expired and a new link is provided to get a new email with an activation link.
3. When the user clicks on that link, the Email Sent Page is displayed.

Business Rules:

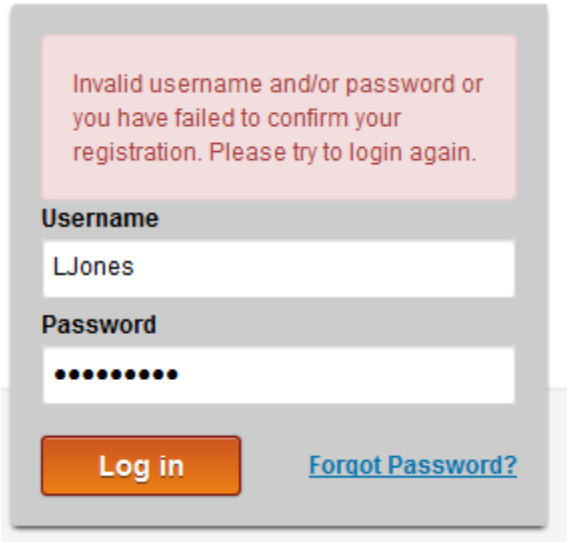
- The trigger TR_AIU_BISC_USER_INFO creates a user in the ImmPort 2 schema.
    1. Creates a user in the ImmPort 2 schema USER_INFO table.
    2. A contract grant is created with the name as first_name || '_' || last_name || '_' || user_id_immport || '_Contract' in the CONTRACT_GRANT_INFO table.
    3. The user is associated to the Contract Grant. (CG_USER_INFO)
    4. A project is created with the name as new.first_name || '_' || :new.last_name || '_Workspace' and it is associated to the Contract Grant that was created in step 2.
    5. The user is associated to the Project.(PROJECT_ASSIGNED_USER)

1.1.5 Manage Access

In order to log into the ImmPort system, a unique user-id is required with a password. These are created during the registration process or creation of an account. The password is restricted to 8-12 characters with one being a numeric value. Appropriate error messages are displayed, if applicable.

1.1.5.1 User Login-Not Validated

The User login – Not Validated depicts the sequence of events for a user that attempts to login without validation.



1.1.5.2 User Login-Not Validated Use Case

The use case describes the process of the user logging in for the first time before he is validated

Actor: Any user

Pre-Conditions: The user is logging in for the first time

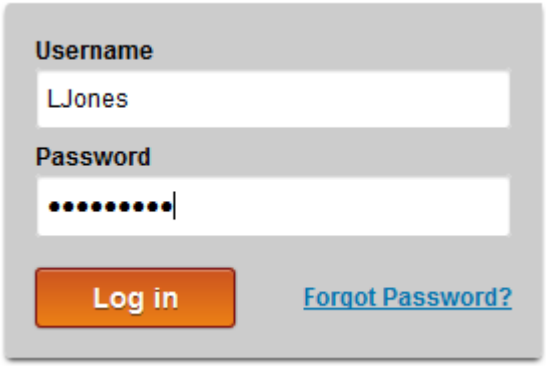
Post- Conditions: An error message is displayed.

Steps:

1. The user accesses the application and logs into the system with his user name and password and clicks on the Login Button.
2. The System finds the user account in the database but it is not yet validated.
3. The system displays the Login Page with an Error message to the user "Invalid user name and password or you have failed to confirm your registration ".

1.1.5.3 User Login

The User Login depicts the sequence for a user to login to the system for the first time after validation.



1.1.5.4 User Login

The use case describes the process of the user logging in for the first time after validation
Actor: Any user

Pre-Conditions: The user is logging in for the first time.

Post- Conditions: The user is logged into the system.

Steps:

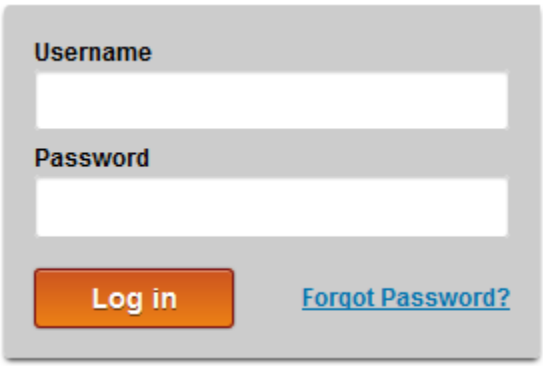
1. The user accesses the application and logs into the system with his/her user login name and password and clicks the Login Button.
2. The System displays the Agreement Screen based on the application.
3. The user clicks on the Continue button.
4. The user is logged into the System.

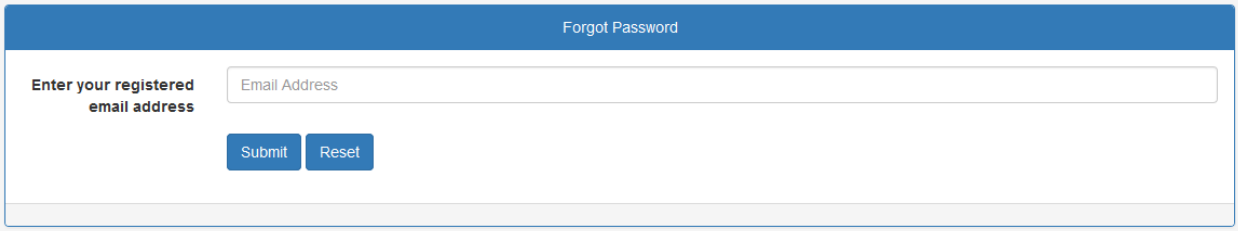
Business Rules:

- NIAID funded applications will be shown the agreement screen.

1.1.5.5 Forgot Password

The Forgot Password Sequence Diagram depicts the sequence of events for a user that has forgotten their username/password.



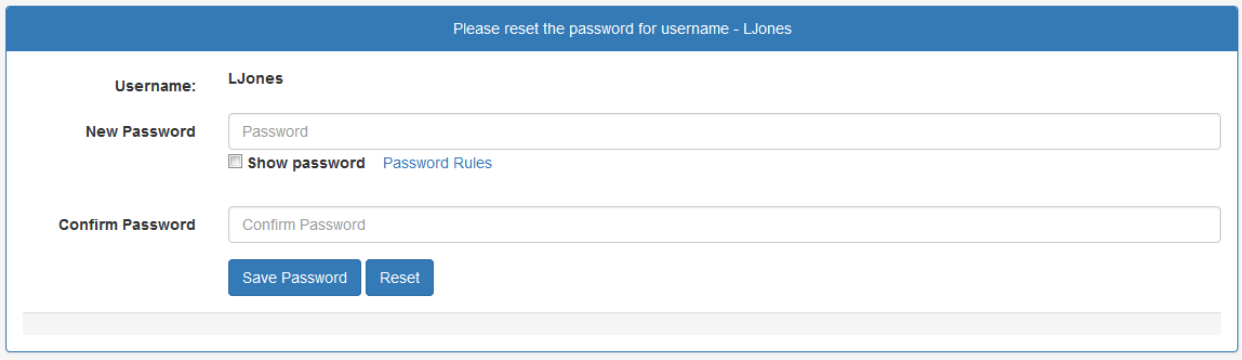


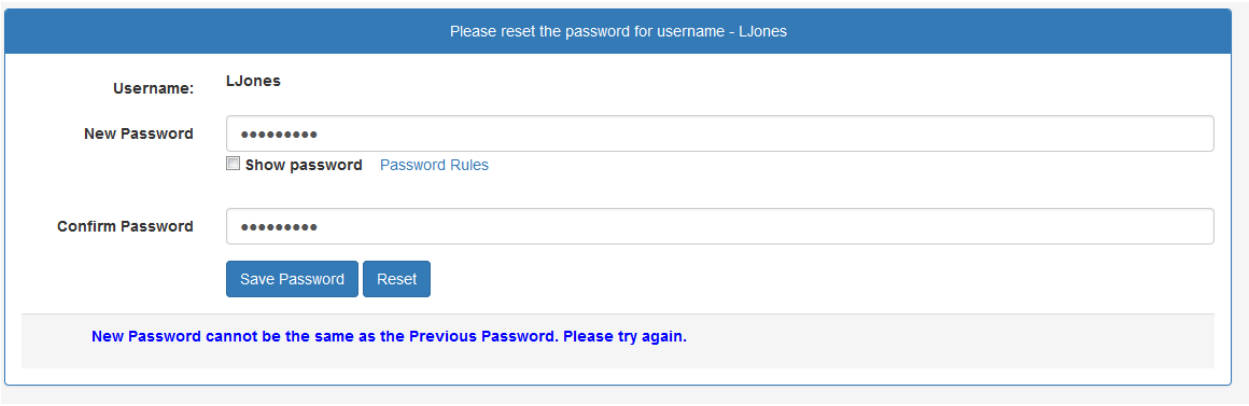
A URL link will be sent to your email account. Please click on the link in the email to reset your password.

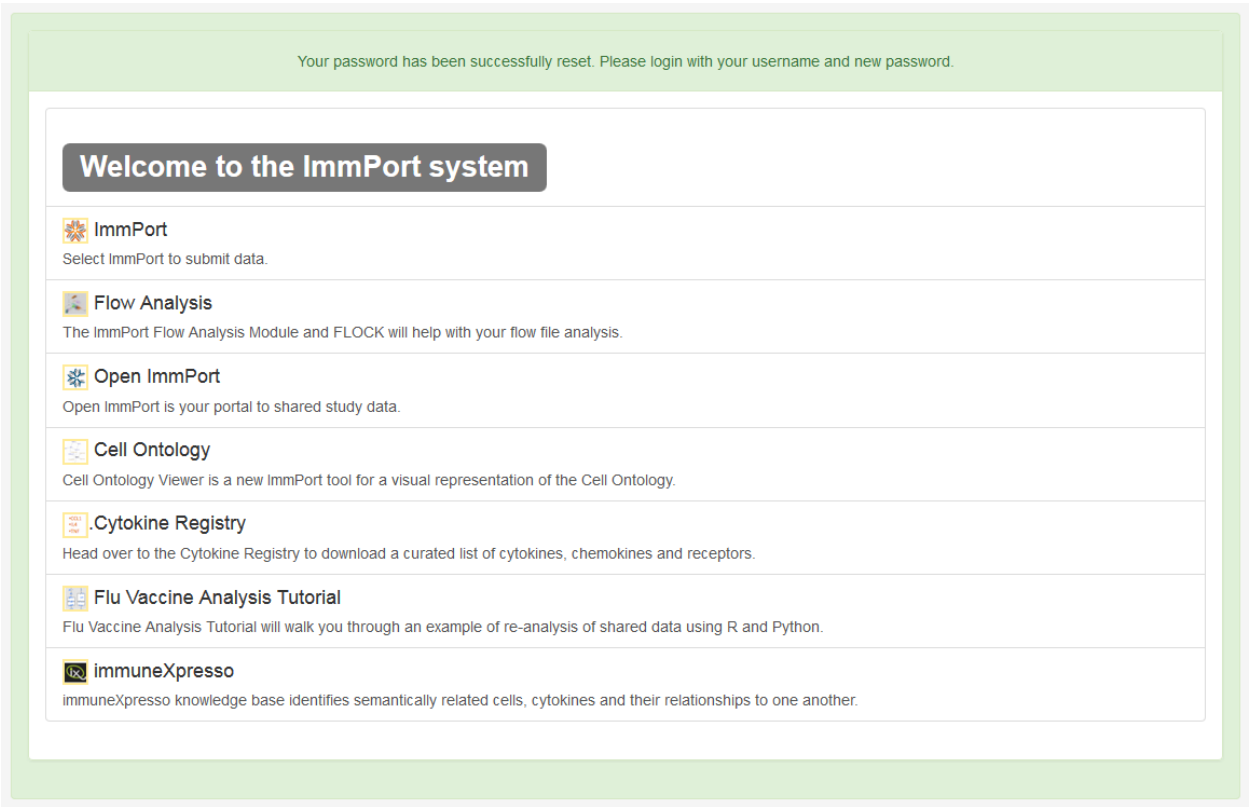
Dear Lynn Jones,

The link below will allow you to reset the password on your ImmPort Account.
Click here to reset your password

This is an automated message. Please do not reply to this email, but contact BISC_HELPDESK@mail.nih.gov if you have any questions.







1.1.5.6 Forgot Password Use Case

The use case describes the process of the user resetting his password pre-login.

Actor: A user who has an account

Pre-Conditions: A valid user.

Post- Conditions: The user is logged into the system.

Steps:

1. The user accesses an application and clicks on the Forgot Password link.

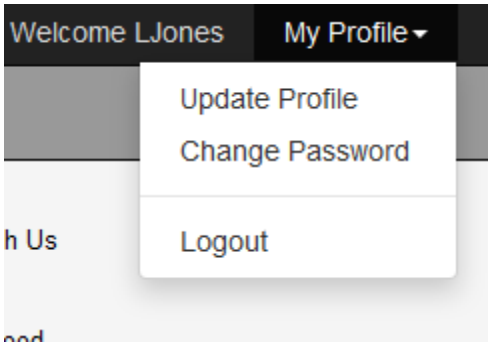
2. The system displays a Forgot Password screen for the user to enter his email address.
3. The user enters his correct email address.
4. The user clicks on the Submit button, a Reset Password Email Link sent to the user's email page is displayed.
5. The system sends the user an email with a Reset Password URL link which contains a unique code.
6. The system changes the status of the user to Pending. The user cannot login to the applications at this point even if he remembers his password.
7. The user clicks on the URL link in his email. A Reset Password page is displayed.
8. The user happens to enter the same password as his previous one. The system displays an error message.
9. The user enters another password then clicks on the Save Password button.
10. The system updates the password and activates the User Account.

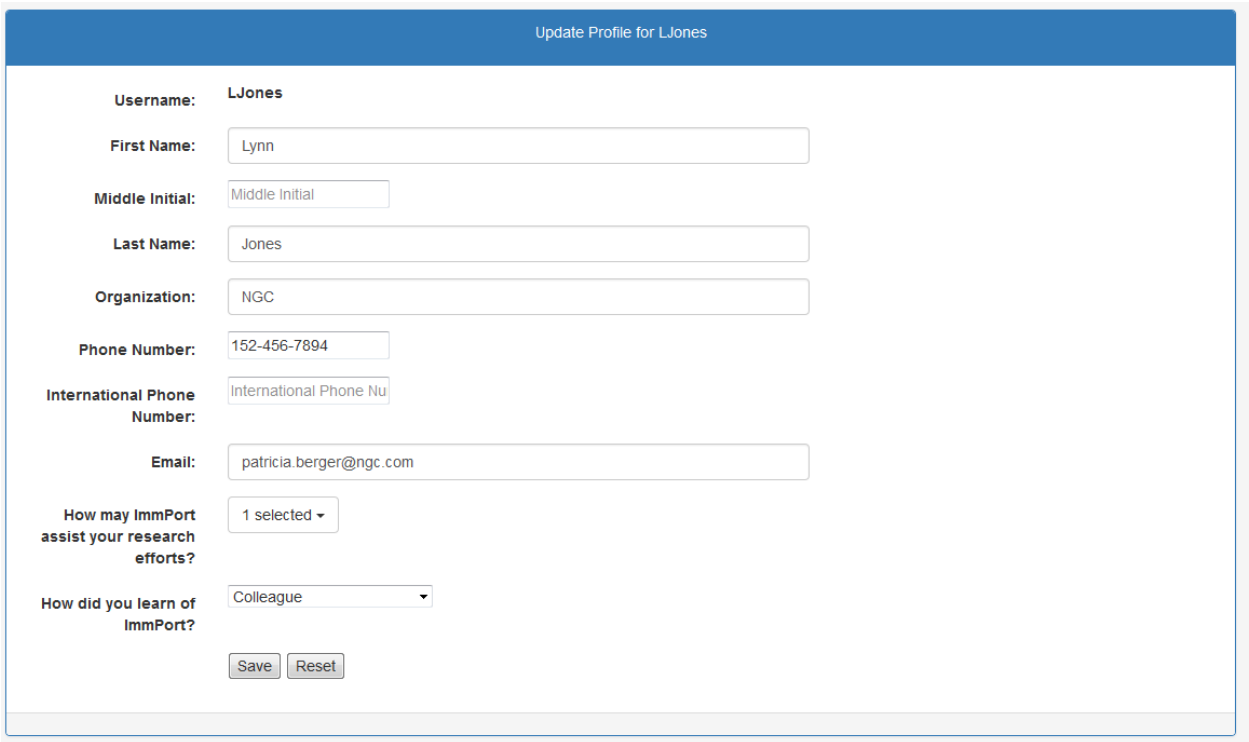
Business Rules:

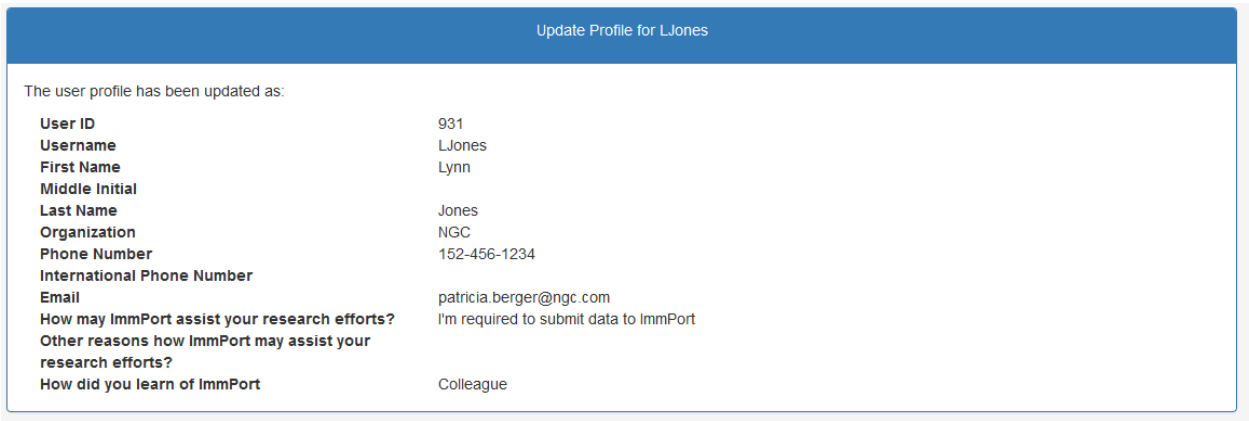
- The URL link that is sent to the user will be valid only for a certain time.
- If the user does not use the URL link within a certain time limit, the link will expire.

1.1.5.7 Update User Profile

The Update User Profile depicts the sequence of events for a user that updates their profile.







1.1.5.8 Update User Profile Use Case

The use case describes the process of updating a specified user profile.

Actor: A user with an account

Pre-Conditions: The user is logged into the system.

Post- Conditions: The user profile is updated in the database.

Steps

1. The user clicks the Update Profile menu in the Security Application or any Other Application.

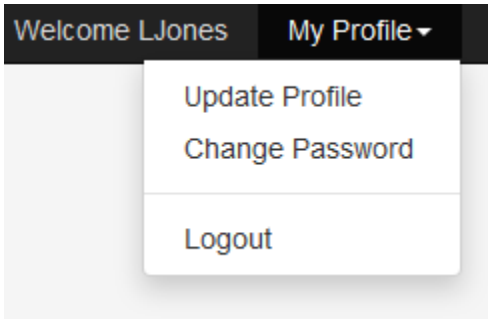
2. The user needs to login to the Security Application if they are coming from any other Application.
3. The "Update User Profile" screen is displayed.
4. The user can update any of the editable data fields
5. The user clicks on “Save” button.
6. The System updates the user information in the database.

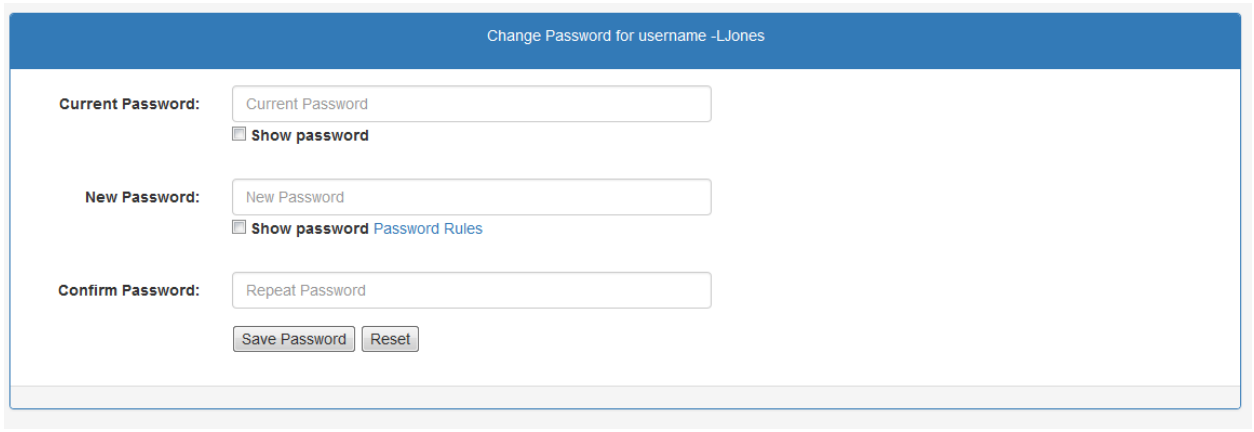
Business Rules:

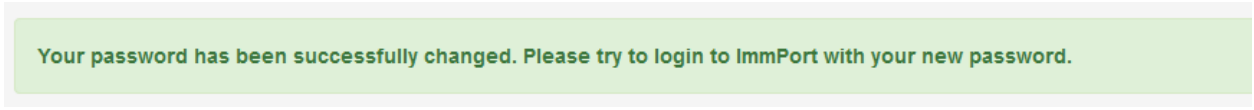
- The email address has to be unique.
- The trigger TR_AIU_BISC_USER_INFO updates the corresponding fields in the DEVELOPER.USER_INFO table.

1.1.5.9 Change Password

The Change Password depicts the sequence of events for a user to change their password.







1.1.5.10 Change Password Use Case

This use case describes the process of changing the password of the logged in user.

Actor: A user with an account.

Pre-Conditions: The user is logged into an Application

Post- Conditions: The user password is updated

Steps:

1. The user clicks the Change Password menu link of the Application they are in.
2. The System displays the Change Password screen.
3. The user clicks on the Change Password button
4. The System updates the user information in the database with the new encrypted password and shows the Change Password Success Page

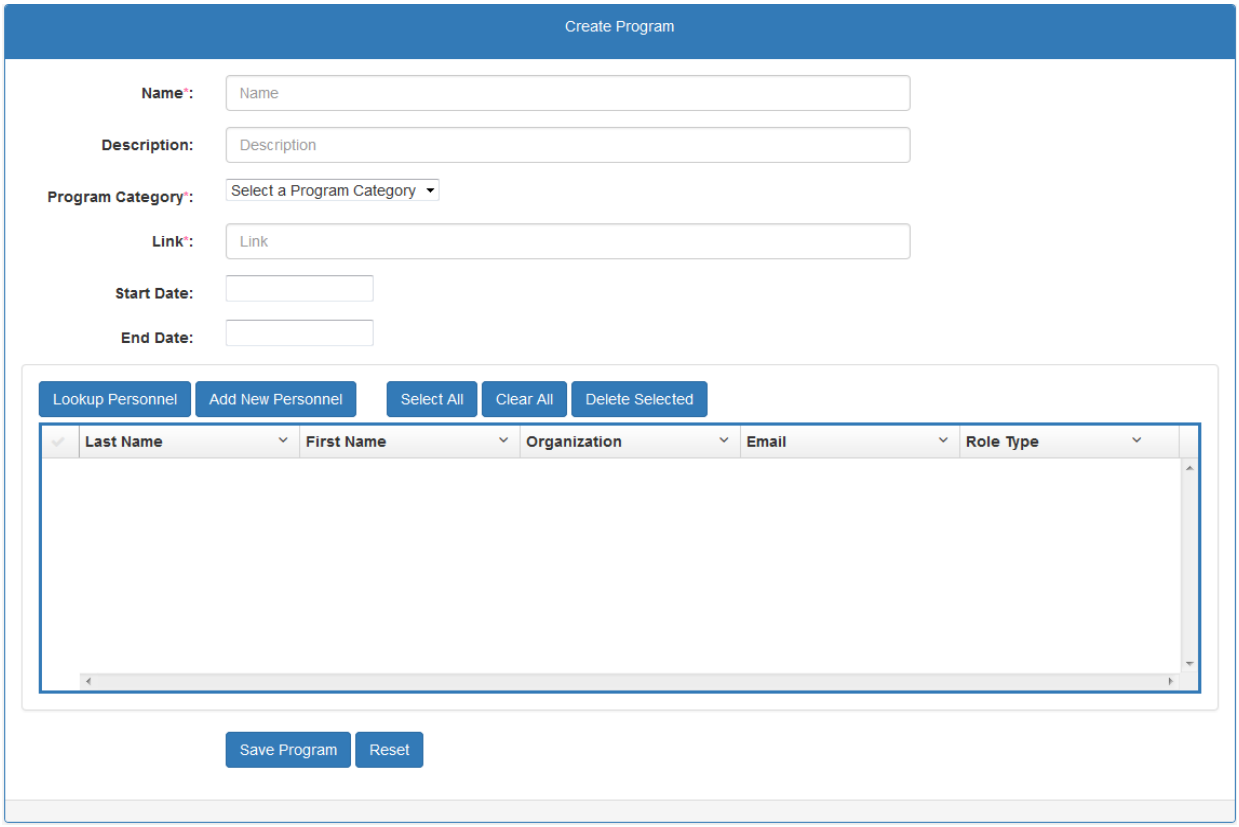
Business Rule:

Current Password and New Password cannot be the same.
The trigger TR_AIU_BISC_USER_INFO updates the corresponding fields in the DEVELOPER.USER_INFO table.

1.2 PROGRAM, CONTRACT, PROJECT MANAGEMENT

1.2.1.1 Create Program

The create program diagrams depict the events for creating a program. Appropriate error messages are displayed if errors are encountered. Once the program is created, contracts are associated.



1.2.1.2 Create Program Use Case

The use case describes the process for creating a Program in the System.

Actor: A user with the BISCAdministrator Role

Pre-Conditions - The user is logged into the System.

Post- Conditions - A Program is created in the database.

Steps:

1. The user accesses the ImmPort 3 Application website and clicks on the Create Program Menu.
2. A "Create Program" screen is displayed.
3. The user enters the data and clicks on the Create Program button.
4. The System creates a new Program in the database.

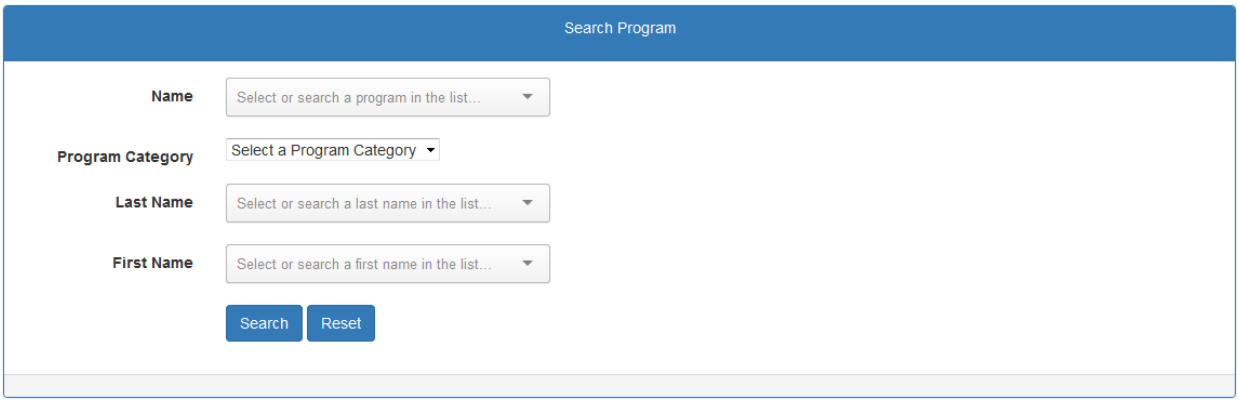
Business Rules:

Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column

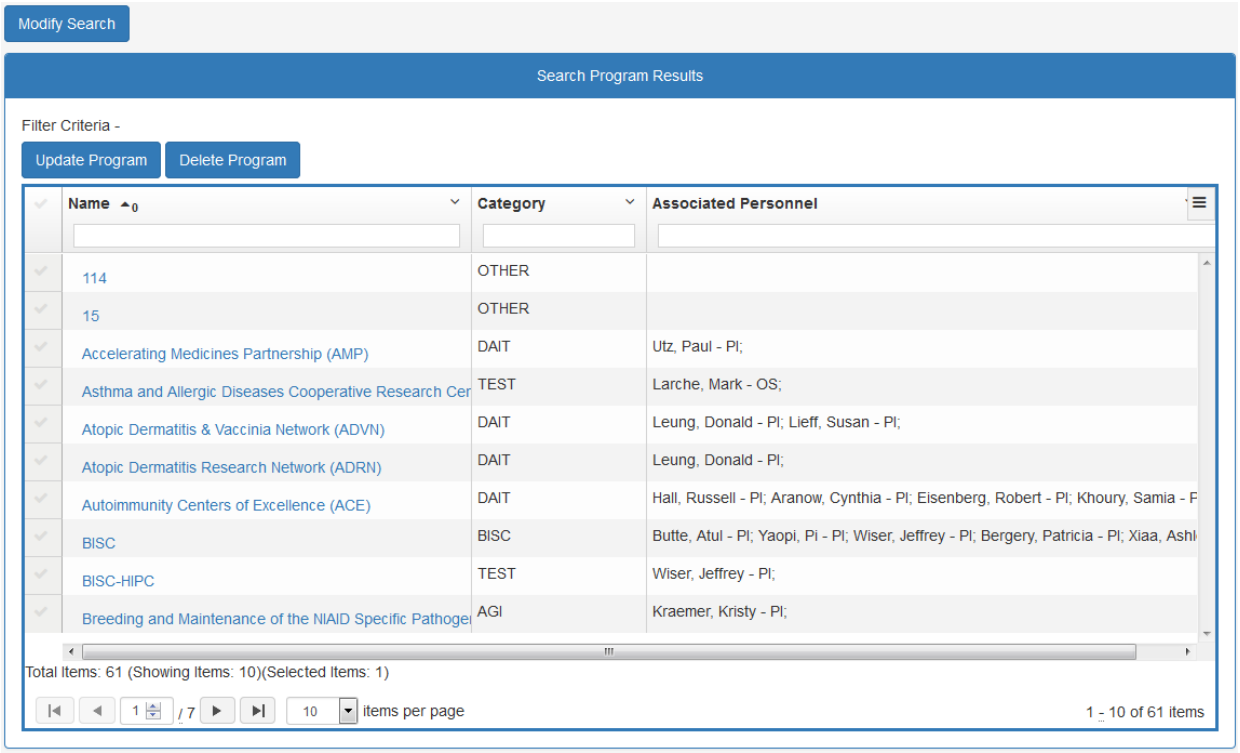
Title	Textbox	Y	Y		Text	PROGRAM_INFO	TITLE
Description	Text area	Y	Y		Text	PROGRAM_INFO	PROGRAM_ABSTRACT
Category	Dropdown	Y	Y	List of Values: LK_PROGRAM_CATEGORY	Text	PROGRAM_INFO	PROGRAM_CATEGORY
Link	textbox	Y	Y			new	new
Start Date	Date	Y	Y		Date	PROGRAM_INFO	START_DATE
End Date	Date	Y	Y		Date	PROGRAM_INFO	END_DATE
Create	Button						
Reset	Button						

1.2.1.3 Search Program

The search program diagrams depict the events for searching a program. Appropriate error messages are displayed if errors are encountered. The user is able to search on the Name, Program Category, Last Name, or First Name.



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Title	Textbox	NA	Y		Text	PROGRAM_INFO	TITLE
Category	Dropdown	NA	Y	List of Values:	Text	PROGRAM_INFO	PROGRAM_CATEGORY
Program/Project Officer(Last Name)	Textbox	NA	Y			PROGRAM_INFO	PROJECT_OFFICER
Search	Button						
Reset	Button						



A list of program search results is displayed. This allows the user to select a program to view or modify. In order to modiy the search, click the "Modify Search" link.

Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Modify Search	Link	NA	NA				
Select Box	Checkbox /List Item	NA	NA				
Title	List Item	NA	NA	Link leads to View Program Details	Text	PROGRAM_INFO	TITLE
Category	List Item	NA	NA		Text	PROGRAM_INFO	PROGRAM_CATEGORY
Program/Project Officer	List Item	NA	NA			PROGRAM_INFO	PROJECT_OFFICER
View Program Details	Button						
Update Program Details	Button						

1.2.1.4 Search Program Use Case

The use case describes the process for searching a program in the System.

Actor: A user with the BISCAdministrator Role.

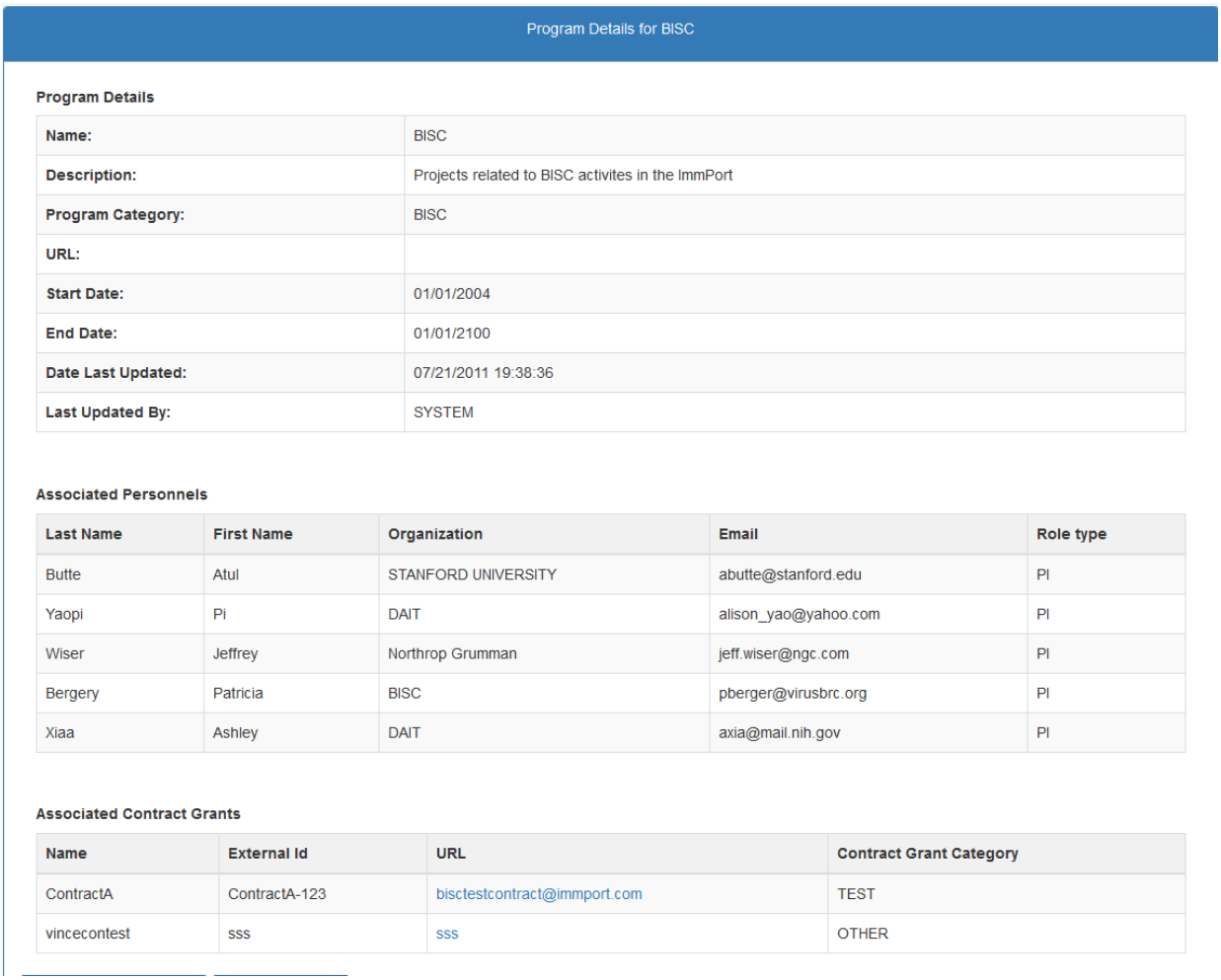
Pre-Conditions - The user is logged into the System.

Post- Conditions - A list of Programs that match the criteria are displayed.

Steps:

1. The user clicks on the Search Program Menu.
2. A "**Search Program**" screen is displayed
3. The user enters the search criteria and clicks on the Submit button.
4. The System displays a list of the Programs that match the criteria on the same page
5. The user can modify the search by clicking Modify Search link. The system clears out the existing search criteria and hides the search results table.
6. The user can select a Program and click on View Program Details button or the Update Program button

1.2.1.5 View Program Details



Program Details for BISC

Program Details

Name:	BISC
Description:	Projects related to BISC activites in the ImmPort
Program Category:	BISC
URL:	
Start Date:	01/01/2004
End Date:	01/01/2100
Date Last Updated:	07/21/2011 19:38:36
Last Updated By:	SYSTEM

Associated Personnels

Last Name	First Name	Organization	Email	Role type
Butte	Atul	STANFORD UNIVERSITY	abutte@stanford.edu	PI
Yaopi	Pi	DAIT	alison_yao@yahoo.com	PI
Wiser	Jeffrey	Northrop Grumman	jeff.wiser@ngc.com	PI
Bergery	Patricia	BISC	pberger@virusbrc.org	PI
Xiaa	Ashley	DAIT	axia@mail.nih.gov	PI

Associated Contract Grants

Name	External Id	URL	Contract Grant Category
ContractA	ContractA-123	bisctestcontract@immport.com	TEST
vincecontest	sss	sss	OTHER

Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column

Title	Textbox	NA	N		Text	PROGRAM_INFO	TITLE
Description	Textbox	NA	N		Text	PROGRAM_INFO	PROGRAM_ABSTRACT
Category	Textbox	NA	N		Text	PROGRAM_INFO	PROGRAM_CATEGORY
Link	textbox	Y	Y			new	new
Start Date	Textbox	NA	N		Date	PROGRAM_INFO	START_DATE
End Date	Textbox	NA	N		Date	PROGRAM_INFO	END_DATE
Program/Project Officer	Textbox	NA	N		Text	PROGRAM_INFO	PROJECT_OFFICER
Deputy Program/Project Officer	Textbox	NA	N		Text	PROGRAM_INFO	DEPUTY_PROJECT_OFFICER
Associated Contracts-Grants	Label	NA	N				
Contract Title	List Item	NA	N				
Contract Id	List Item	NA	N				
Contract URL	List Item	NA	N				
Update Program Details	Button						

The use case describes the details of the Program Details screen.

Actor: A user with the BISCAdministrator Role

Pre-Conditions - The user has clicked the View Program Details button on the Search Program screen or on the Title link.

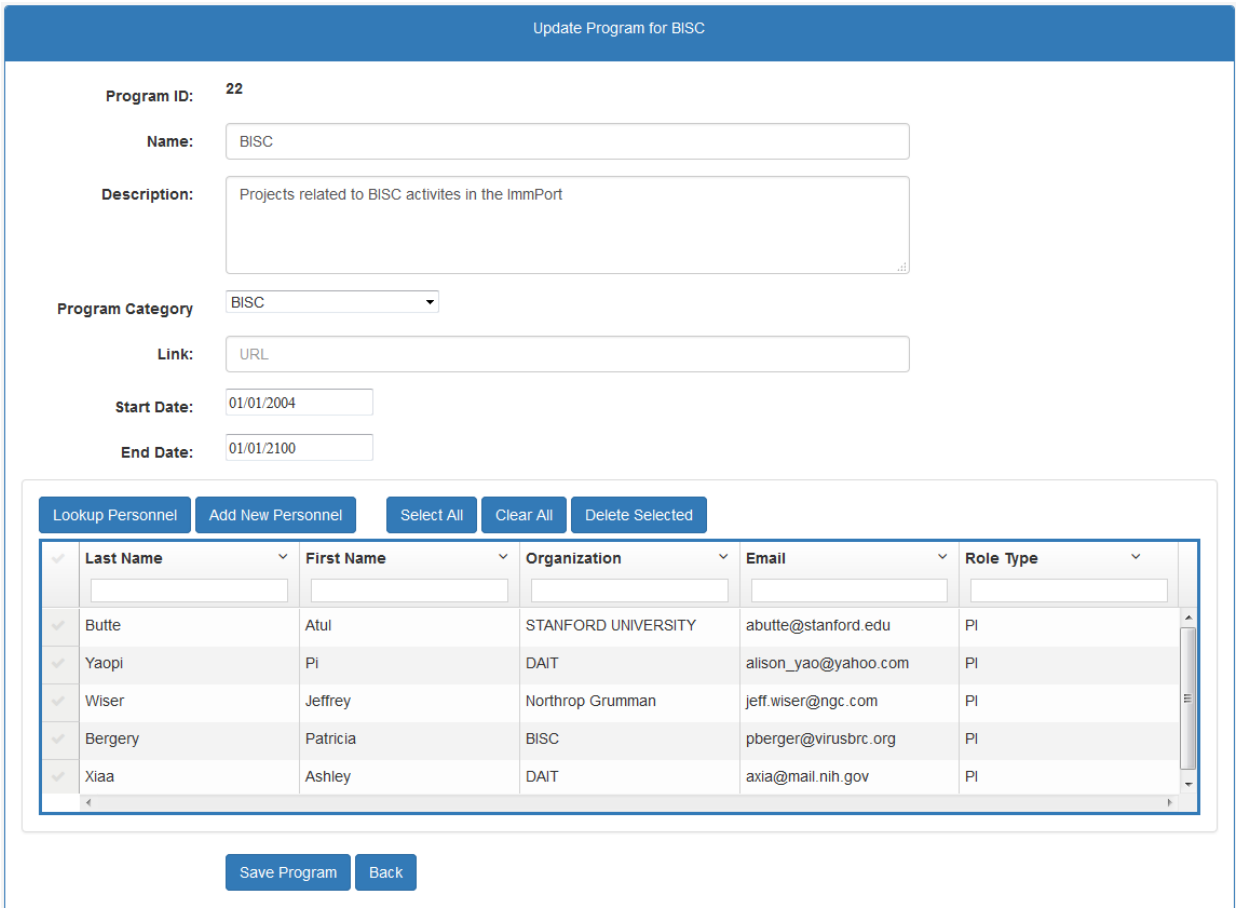
Post- Conditions - The program details are displayed.

Steps:

1. A "Program Details " screen is displayed
2. The user clicks on the Update Program button.
3. The "Update Program Details" screen is displayed.

1.2.1.6 Update Program

The Update Program diagrams depict the events for updating a program. Appropriate error messages are displayed if errors are encountered.



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Title	Textbox	Y	Y		Text	PROGRAM_INFO	TITLE
Description	Text area	Y	Y		Text	PROGRAM_INFO	PROGRAM_ABSTRACT
Category	Dropdown	Y	Y		Text	PROGRAM_INFO	PROGRAM_CATEGORY
Link	textbox	Y	Y			new	new
Start Date	Date	Y	Y		Date	PROGRAM_INFO	START_DATE
End Date	Date	Y	Y		Date	PROGRAM_INFO	END_DATE
Program/Project Officer	Lookup	Y	Y		Text	PROGRAM_INFO	PROJECT_OFFICER
Deputy Program/Project Officer	Lookup	N	Y		Text	PROGRAM_INFO	DEPUTY_PROJECT_OFFICER
Save	Button						
Reset	Button						

The Contracts-Grants are associated to the project. Click on a Contract-Grant title to view the details	Label						
Associated Contracts-Grants	Label	NA	N				
Contract Title	List Item	NA	N				
Contract Id	List Item	NA	N				
Contract URL	List Item	NA	N				
Add	Lookup			The lookup will allow the user select a Contract- Grant and add it to the Program. This Contract Grant will be disassociated from the existing Program it belongs to and will be associated to the current Program			

1.2.1.7 Update a Program Class Diagram

The use case describes the process of updating a Program.

Actor: A user with the BISCAdministrator Role

Pre-Conditions - The user has clicked the Update Program button on the View Program Detail screen or on the "Search Program" screen.

Post- Conditions - The program details are updated in the database.

Steps:

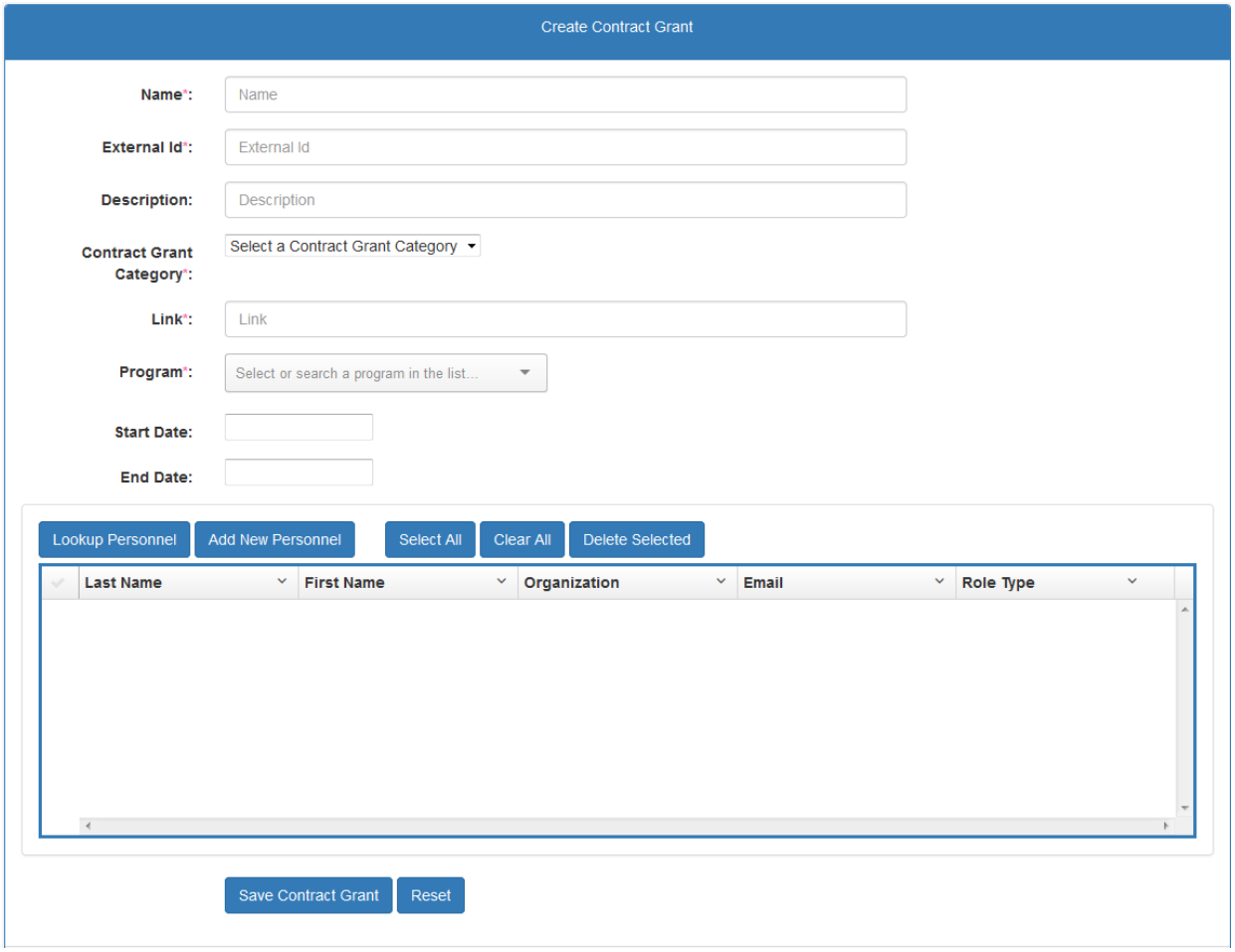
1. The user modifies the data on the "Update Program Details" screen.
2. The user can associate the Program to new contract-grants.
3. The user clicks on the Update Program button.
4. The System updates the data in the database.

Business Rules:

1. **IMM3-ADM-BR3 -** The Contract Grants being added to this Program will be disassociated from the existing Program that they belong to and will be associated to the current Program.

1.2.1.8 Create Contract Grant

The Add/Update Contract diagrams depict the events for adding and updating a contract. Appropriate error messages are displayed if errors are encountered. Once the contract is added, a Principal Investigator, Program Mananger and Other Staff is associated with the contract. Once the associated users are added, a default project may be created. The associated users to the contract will obtain access to the default project.



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Title	Textbox	Y	Y		Text	CONTRACT_GRANT_INFO	TITLE
Contract-Grant	Textbox	Y	Y		Text	CONTRACT_GRANT_INFO	CG_NUMBER

Number							
Link	Textbox	N	Y			new	new
Abstract	Text area	Y	Y		Text	CONTRACT_GRANT_INFO	CG_ABSTRACT
Category	Dropdown	Y	Y	List of Values: LK_CG_CATEGORY	Text	CONTRACT_GRANT_INFO	CG_CATEGORY
Start Date	Date	Y	Y		Date	CONTRACT_GRANT_INFO	START_DATE
End Date	Date	Y	Y		Date	CONTRACT_GRANT_INFO	END_DATE
Program	Dropdown	Y	Y	The list of programs in the System	Number	CONTRACT_GRANT_INFO	PROGRAM_ID
Create Contract-Grant	Button						

The use case describes the process of creating a Contract-Grant.

Actor: A user with the BISCAdministrator Role

Pre-Conditions - The user is logged into the System.

Post- Conditions - A contract-grant is created in the database

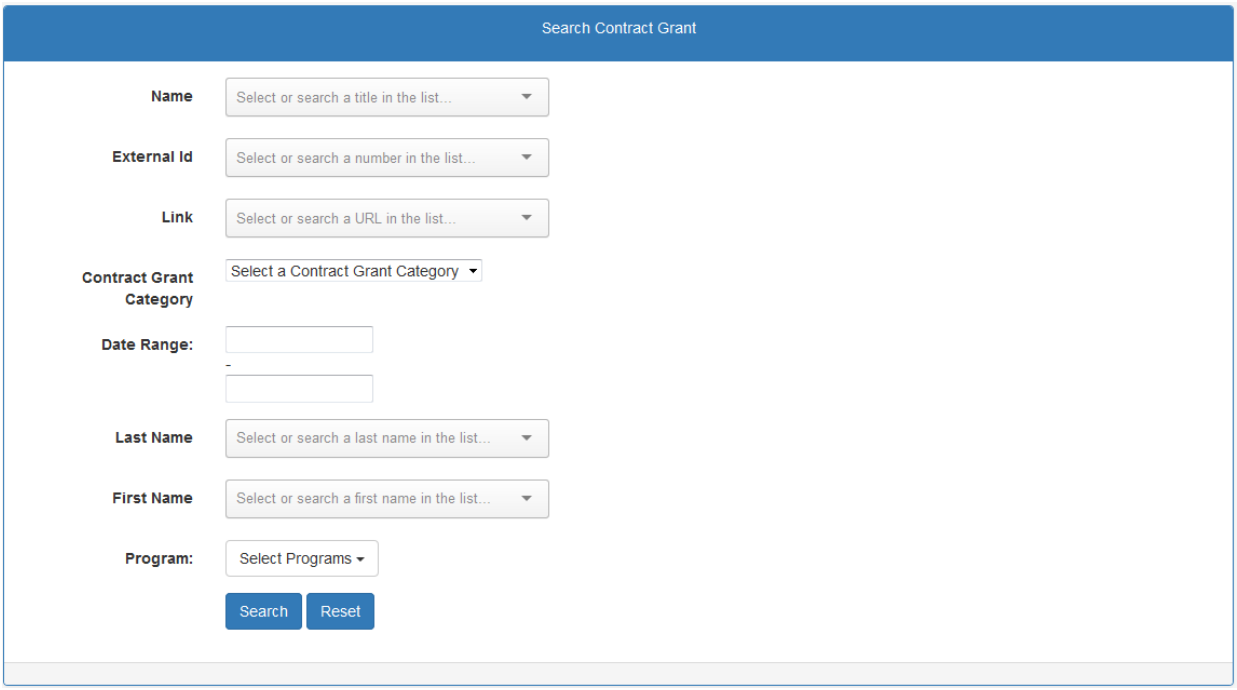
Steps:

1. A "Create Contract-Grant" screen is displayed.
2. The user enters data and also selects a Program to associate the Contract-Grant.
3. The user clicks on the Submit button.
4. The system creates a contract-grant in the database associates it the selected Program

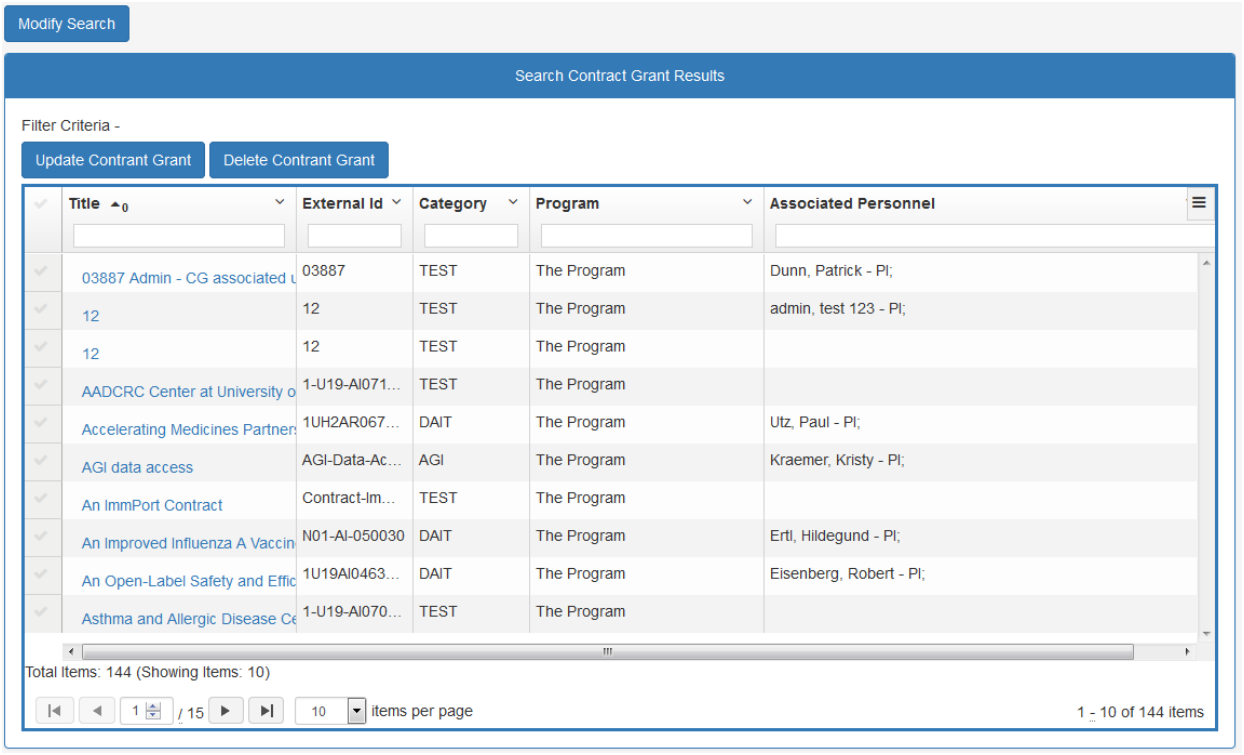
Business Rules:

1.2.1.9 Search Contract Grant

The Search Contract diagrams depict the events for searching a contract. Appropriate error messages are displayed if errors are encountered. A user is able to search on the fields Title, Grant – Contract Number, Category, Start Date, End Date, ImmPort Access End Date, Principal Investigator, Associated Program Name or Status.



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Title	Textbox	NA	Y		Text	CONTRACT_GRANT_INFO	TITLE
Contract-Grant Number	Textbox	NA	Y		Text	CONTRACT_GRANT_INFO	CG_NUMBER
Contract-Grant Category	Dropdown	NA	Y		Text	CONTRACT_GRANT_INFO	CG_CATEGORY
Date Range	Two Date Fields	NA	Y	Check if the start date is in the range given	Date	CONTRACT_GRANT_INFO	START_DATE
Associated Program Name	Multi-Select List box	NA	Y			CONTRACT_GRANT_INFO	PROGRAM_ID
Search	Button						
Reset	Button						



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Modify Search	Link	NA	NA				
Select Box	Checkbox /List Item	NA	NA				
Contract-Grant Number	List Item/Link	NA	NA	Clicking on the link displays the Contract-Grant details	Text	CONTRACT_GRANT_INFO	CG_NUMBER
Title	List Item	NA	NA		Text	CONTRACT_GRANT_INFO	TITLE
Category	List Item	NA	NA		Text	CONTRACT_GRANT_INFO	CG_CATEGORY
Program	List Item	NA	NA		Number	CONTRACT_GRANT_INFO	PROGRAM_ID
Principal Investigator	List Item	NA	NA			new	new
End Date	List Item	NA	NA		Date	CONTRACT_GRANT_INFO	END_DATE
View Contract-Grant Details	Button						
Update Contract-Grant	Button						

The use case describes the process of searching for a specific Contract-Grant.

Actor: A user with the BISCAdministrator Role

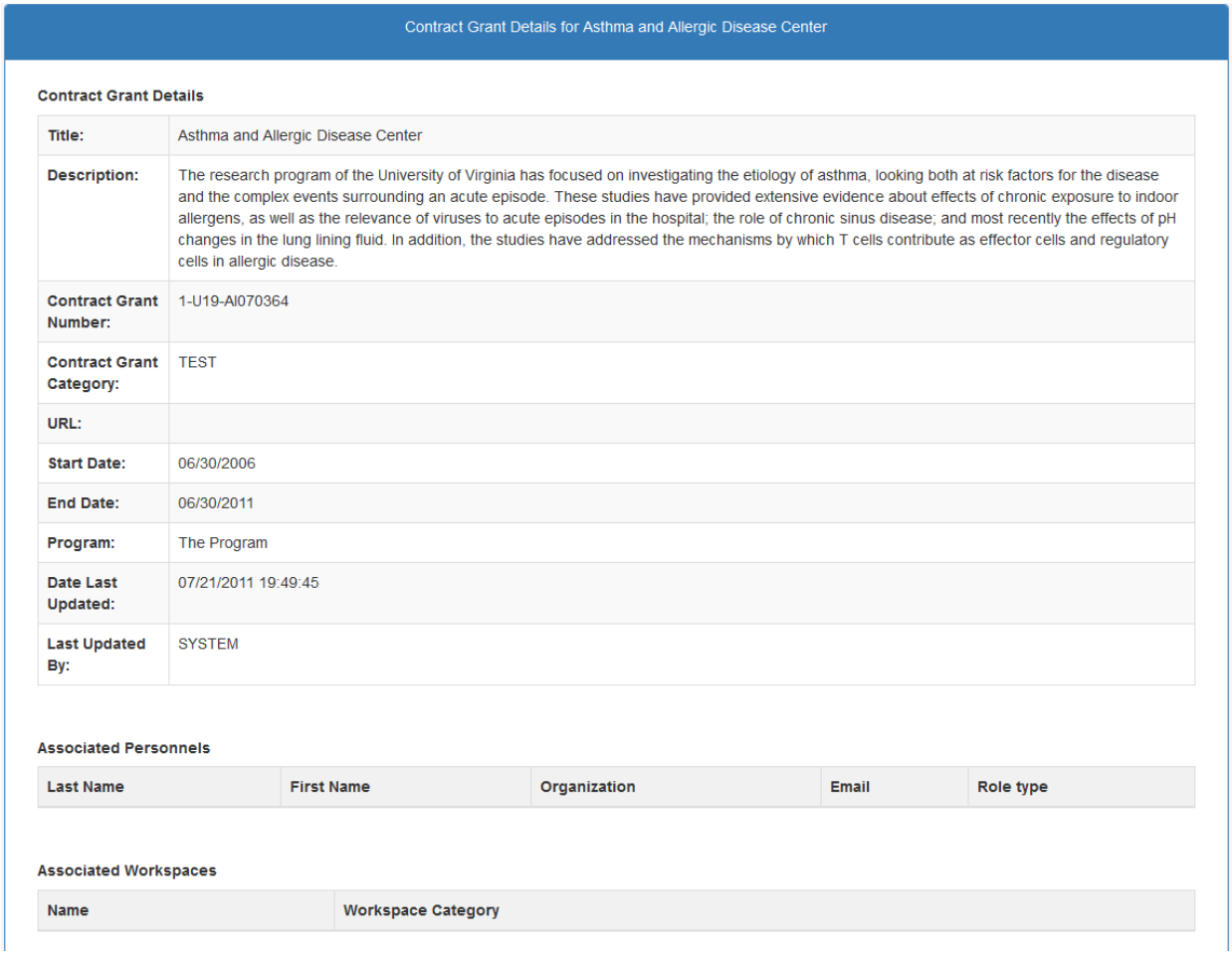
Pre-Conditions - The user is logged into the System.

Post- Conditions - A list of contract-grants matching the criteria are displayed.

Steps:

1. A "**Search Contract-Grant**" screen is displayed.
2. The user enters the search criteria and clicks on the Search button.
3. The user clicks on the Search button.
4. The system displays a list of Contract-Grants that match the criteria.
5. The user can select a specific Contract-Grant and click on the View Contract-Grant Details or Update Contract-Grant button.

1.2.1.10 View Contract Grant


Contract Grant Details for Asthma and Allergic Disease Center

Contract Grant Details

Title:	Asthma and Allergic Disease Center
Description:	The research program of the University of Virginia has focused on investigating the etiology of asthma, looking both at risk factors for the disease and the complex events surrounding an acute episode. These studies have provided extensive evidence about effects of chronic exposure to indoor allergens, as well as the relevance of viruses to acute episodes in the hospital; the role of chronic sinus disease; and most recently the effects of pH changes in the lung lining fluid. In addition, the studies have addressed the mechanisms by which T cells contribute as effector cells and regulatory cells in allergic disease.
Contract Grant Number:	1-U19-AI070364
Contract Grant Category:	TEST
URL:	
Start Date:	06/30/2006
End Date:	06/30/2011
Program:	The Program
Date Last Updated:	07/21/2011 19:49:45
Last Updated By:	SYSTEM

Associated Personnels

Last Name	First Name	Organization	Email	Role type

Associated Workspaces

Name	Workspace Category

Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Title	Textbox	NA	N		Text	CONTRACT_GRANT_INFO	TITLE
Contract-Grant Number	Textbox	NA	N		Text	CONTRACT_GRANT_INFO	CG_NUMBER
URL	Textbox	NA	N		Text	new	new
Abstract	Text area	NA	N		Text	CONTRACT_GRANT_INFO	CG_ABSTRACT
Category	Dropdown	NA	N	List of Values: ???	Text	CONTRACT_GRANT_INFO	CG_CATEGORY
Start Date	Date	NA	N		Date	CONTRACT_GRANT_INFO	START_DATE
End Date	Date	NA	N		Date	CONTRACT_GRANT_INFO	END_DATE
Program	Dropdown	NA	N	The list of programs in the System	Number	CONTRACT_GRANT_INFO	PROGRAM_ID
Program/Project Officer	Lookup	NA	N		Text	CONTRACT_GRANT_INFO	PROJECT_OFFICER
Deputy Program/Project Officer	Lookup	NA	N		Text	CONTRACT_GRANT_INFO	DEPUTY_PROJECT_OFFICER
Associated Workspaces	Label						
Update Contract-Grant	Button						

The use case describes the details of a Contract-Grant Details screen.

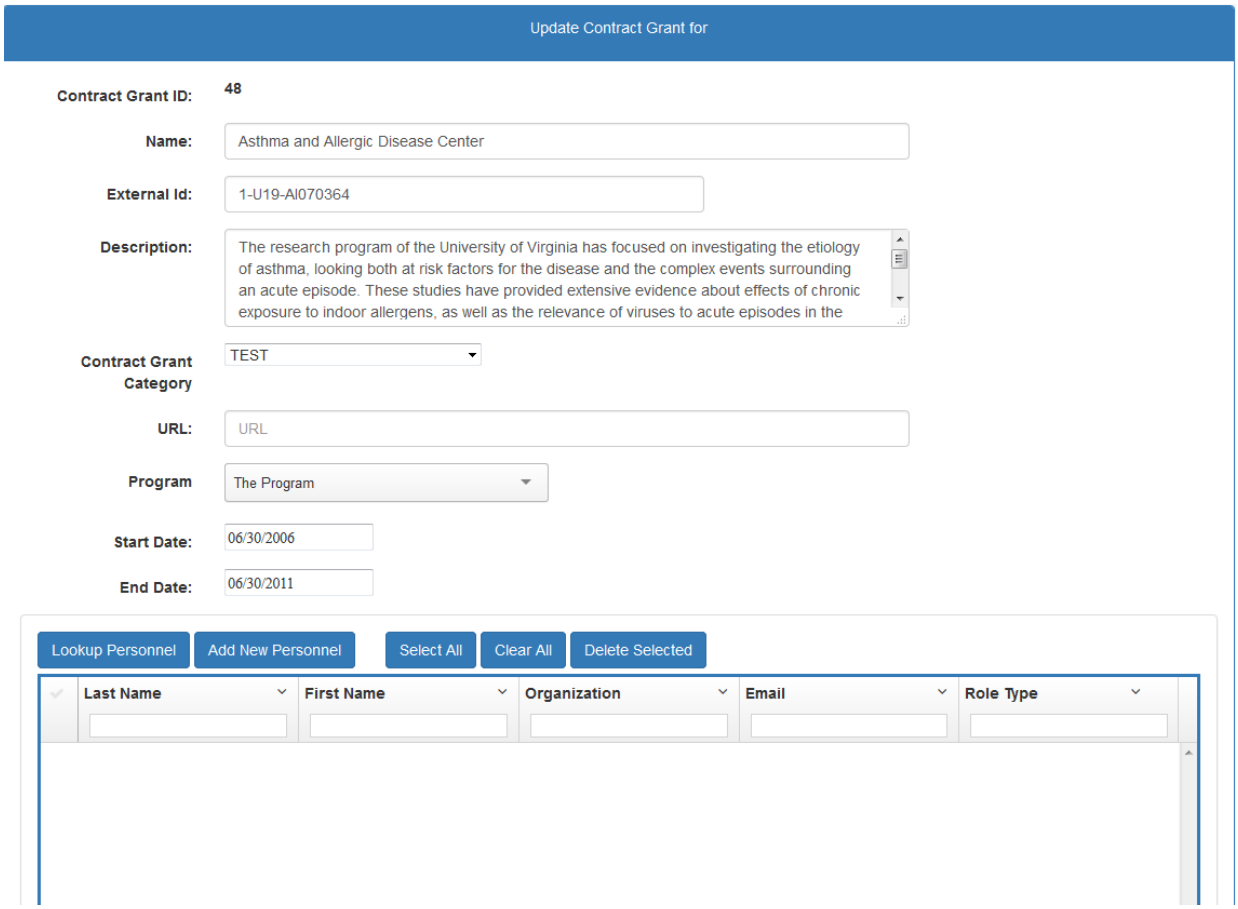
Actor: A user with the BISCAdministrator Role

Pre-Conditions - The user has clicked the View Contract-Detail Details button on the Search Program screen.

Post- Conditions - The contract-grant details are displayed of the select contract-grant.
Steps:

1. A **"Contract-Detail Details**" screen is displayed.

1.2.1.11 Update Contract Grant



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Title	Textbox	Y	Y		Text	CONTRACT_GRANT_INFO	TITLE
Contract-Grant Number	Textbox	Y	Y		Text	CONTRACT_GRANT_INFO	CG_NUMBER
URL					Text	new	new
Abstract	Text area	Y	Y		Text	CONTRACT_GRANT_INFO	CG_ABSTRACT
Category	Dropdown	Y	Y	List of Values: ???	Text	CONTRACT_GRANT_INFO	CG_CATEGORY
Start Date	Date	Y	Y		Date	CONTRACT_GRANT_INFO	START_DATE
End Date	Date	Y	Y		Date	CONTRACT_GRANT_INFO	END_DATE
Program	Dropdown	Y	Y	The list of programs in the System	Number	CONTRACT_GRANT_INFO	PROGRAM_ID
Program/Project Officer	Lookup	Y	Y		Text	CONTRACT_GRANT_INFO	PROJECT_OFFICER
Deputy Program/Project Officer	Lookup	N	Y		Text	CONTRACT_GRANT_INFO	DEPUTY_PROJECT_OFFICER
Update Contract-	Button						

Grant							

The use case describes the process of updating Contract-Grant screen.

Actor: A user with the BISCAdministrator Role

Pre-Conditions - The user has clicked the Update Contract-Grant button on the View Contract-Grant Details screen or the "Search Contract-Grant" screen.

Post- Conditions - The contract-grant details are updated in the database.

Steps:

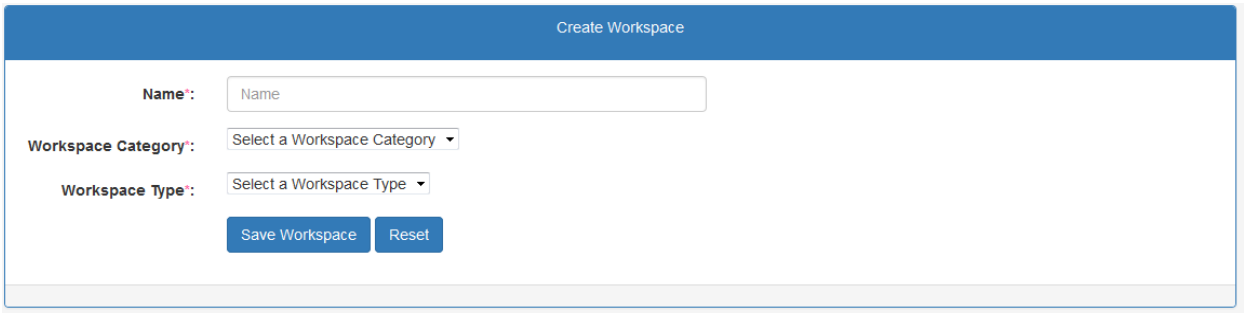
1. The user modifies the data on the "**Update Contract-Grant**" screen.
2. The user can associate the Contract-Grant to a new Program.
3. The user clicks on the Update Contract-Grant button.
4. The System updates the data in the database.

Business Rules:

1. **IMM3-ADM-BR5** - The Contract Grants being will be disassociated from the existing Program that it belongs to and will be associated to the selected Program.

1.2.1.12 Create Workspace

The Add/Update project diagrams depict the events for adding and updating a project. Appropriate error messages are displayed if errors are encountered.



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Title	Textbox	Y	Y		Text	RESEARCH_PROJECT_INFO	TITLE
Category	Dropdown	Y	Y	List of Values are : LK_PROJECT_CATEGORY	Text	RESEARCH_PROJECT_INFO	PROJECT_CATEGORY
Contract-Grant	Multi-select	Y	Y		Number	RESEARCH_PROJECT_INFO	CG_ID
Associated Users						PROJECT_ASSIGNED_USER	
Name	List Item	NA	N			USER_INFO	FIRST_NAME, LAST_NAME

Phone	List Item	NA	N			USER_INFO	PHONE_NUMBER
Organization	List Item	NA	N			USER_INFO	INSTITUTION
Email	List Item	NA	N			USER_INFO	EMAIL_ADDRESS
Add User	Lookup	N	Y	Clicking the Add User opens a Dialog box with a list of users. Select Multiple users and click Add			
Save	Button						

The use case describes the process of creating a Private Project Workspace.

Actor: A user with the **role** BISCAdministrator role.

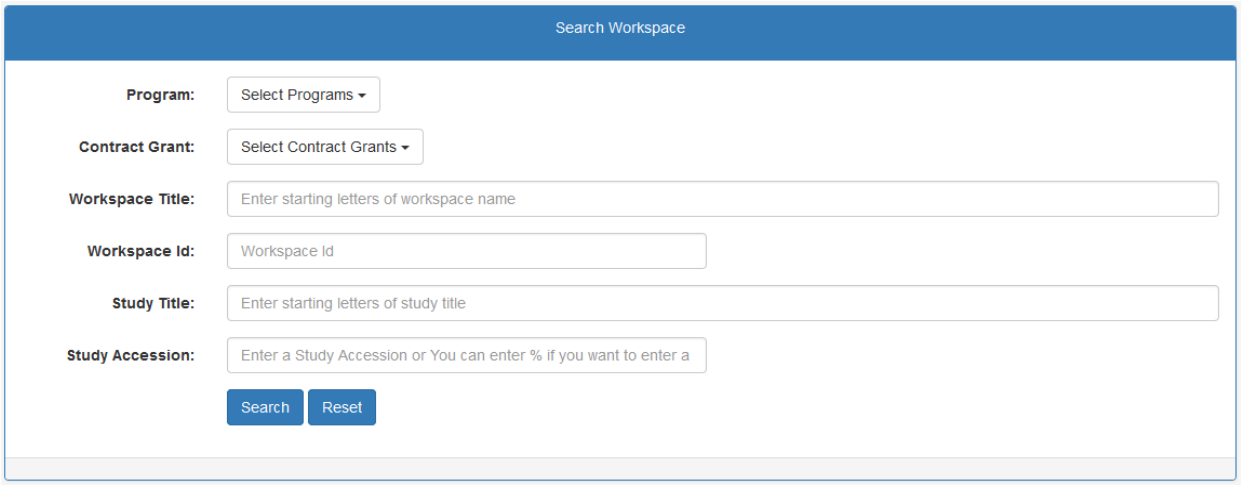
Pre-Conditions - The user has logged in to the Immport3.

Post- Conditions - The system creates a Private Project Workspace in the database.

Steps:

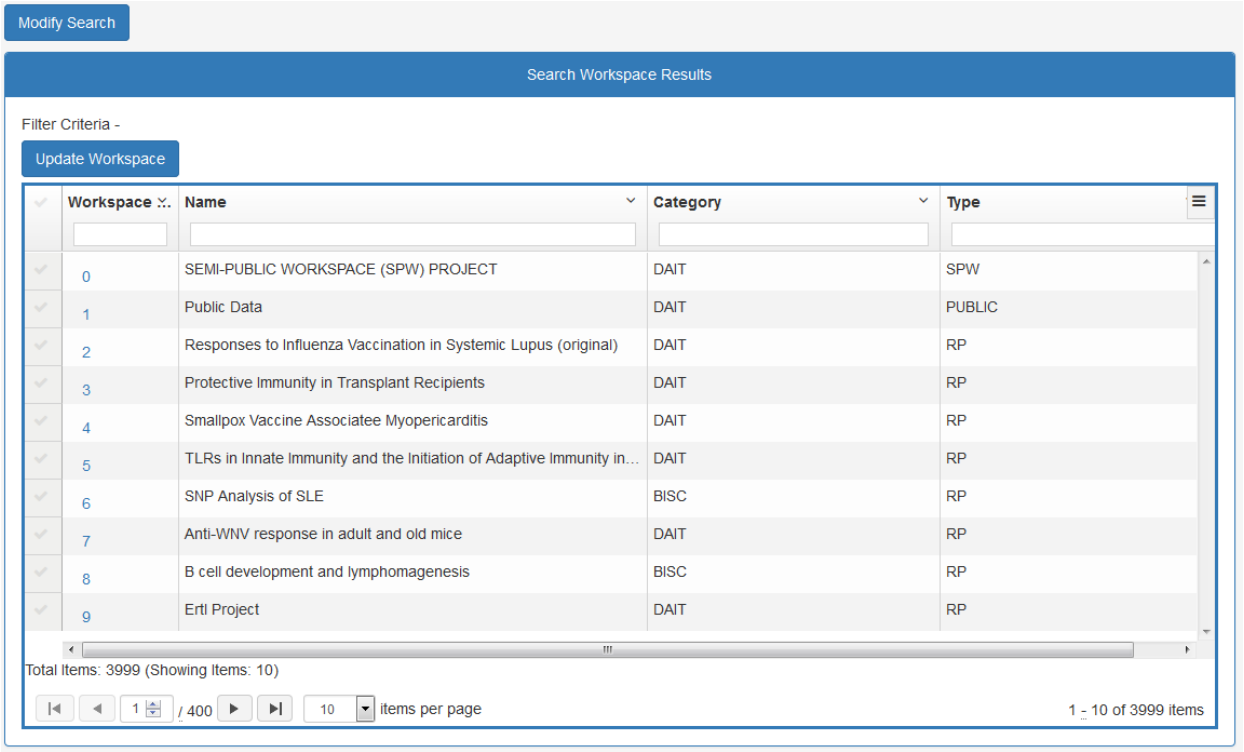
1. The user clicks on the Create Private Project Workspace menu.
2. The "**Create Private Project Workspace**" screen is displayed.
3. The user enters data, selects Contract-Grants and adds users.
4. The System creates a Private Project Workspace.

1.2.1.13 Search Workspace



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Program	Dropdown	NA	Y	List of Programs			
Contract-Grants	Lookup	NA	Y	Accepts %			

Project Title	lookup	NA	Y	Can take %			
Project ID	Textbox	NA	Y	Can take %			
Search	Button						
Reset	Button						



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Modify Search	Link	NA	NA				
Select Box	Checkbox /List Item	NA	NA				
Project Title	List Item/Link	NA	NA	Clicking on the link displays the Research Project details	Text	RESEARCH_PROJECT_INFO	TITLE
Project Category	List Item	NA	NA		Text	RESEARCH_PROJECT_INFO	PROJECT_CATEGORY
Project Contract-Grant						RESEARCH_PROJECT_INFO	CG_ID(Multiple)
Project Id						RESEARCH_PROJECT_INFO	PROJECT_ID
View Private Project Workspace Details	Button						
Update	Button						

Private Project Workspace							

The use case describes the process of searching for a Private Project Workspace.

Actor: A user with the **role** BISCAdministrator role

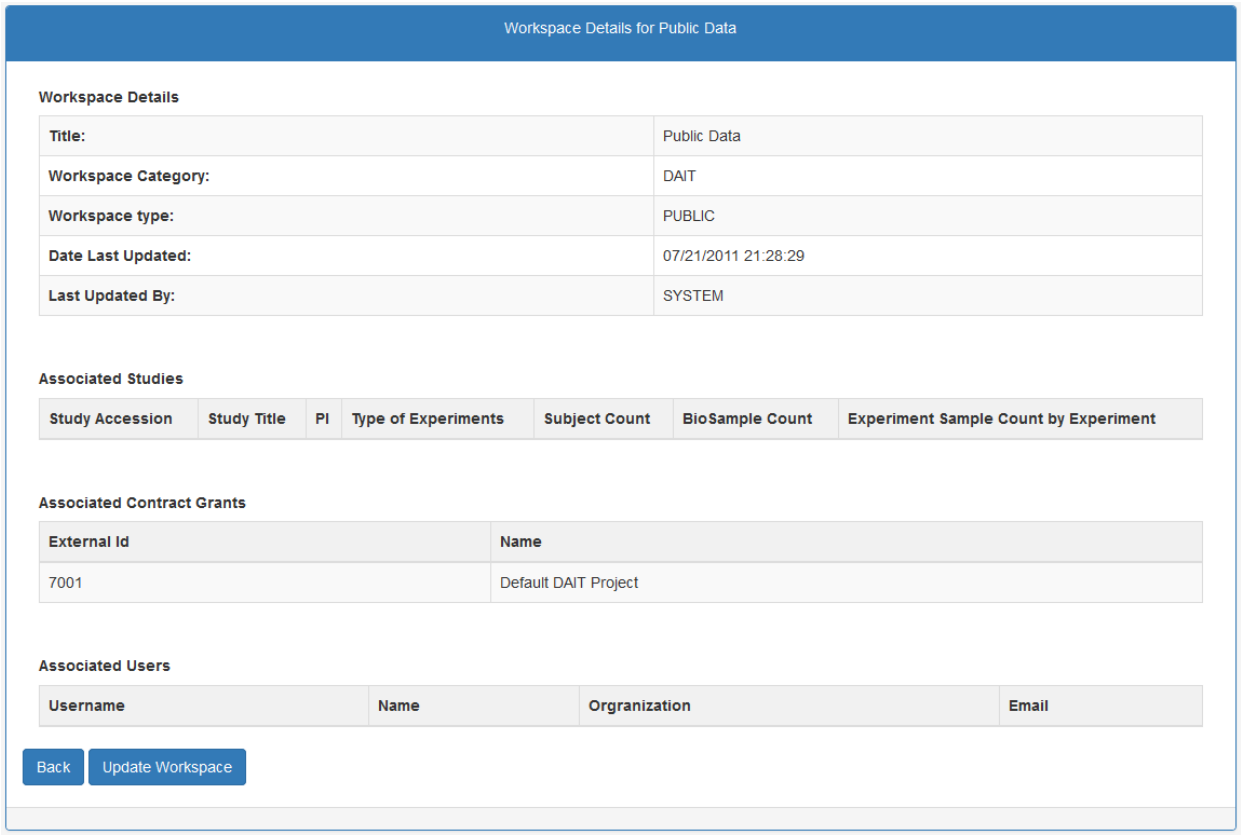
Pre-Conditions - The user has logged in to the Immport3.

Post- Conditions - The system displays the Private Project Workspaces that match the given criteria.

Steps:

1. A "**Search Private Project Workspace**" screen is displayed.
2. The user enters the search criteria and clicks on the Search button.
3. The user clicks on the Search button.
4. The system displays a list of Private Project Workspaces that match the criteria.
5. The user can select a specific Private Project Workspace and click on the View Private Project Workspace Details or Update Private Project Workspace button

1.2.1.14 View Workspace



Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Title	Textbox	NA	N		Text	RESEARCH_PROJECT_INFO	TITLE
Category	Textbox	Textbox	N		Text	RESEARCH_PROJECT_INFO	PROJECT_CATEGORY
Associated Contract-Grants	Label					RESEARCH_PROJECT_INFO	CD_IDs
Contract-Grant Number	Textbox	NA	N			CONTRACT_GRANT_INFO	CG_NUMBER
Contract-Grant Title	Textbox	NA	N			CONTRACT_GRANT_INFO	TITLE
Associated Users	Label					PROJECT_ASSIGNED_USER	
Name	List Item	NA	N			USER_INFO	FIRST_NAME, LAST_NAME
Phone	List Item	NA	N			USER_INFO	PHONE_NUMBER
Organization	List Item	NA	N			USER_INFO	INSTITUTION
Email	List Item	NA	N			USER_INFO	EMAIL_ADDRESS

The use case describes the details of a Private Project Workspace Details screen.

Actor: A user with the BISCAdministrator Role

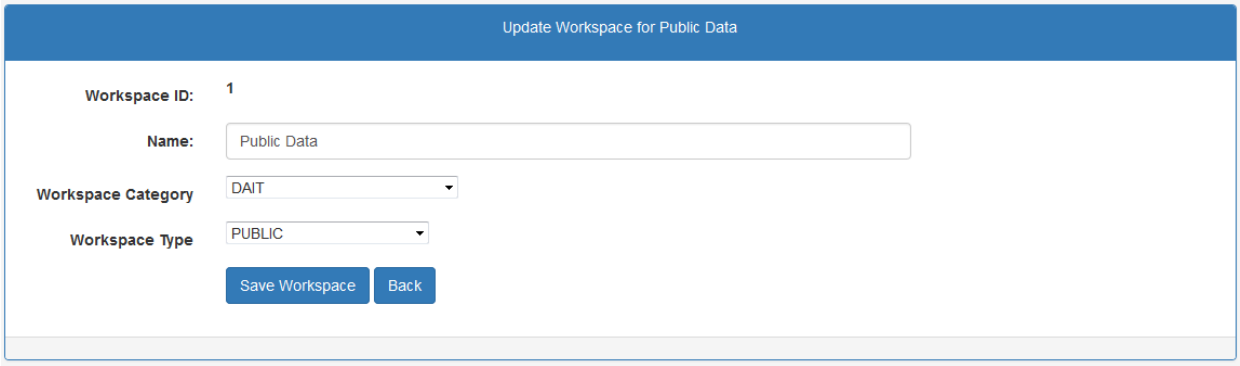
Pre-Conditions - The user has clicked the View Private Project Workspace Details button on the Search Private Project Workspace screen.

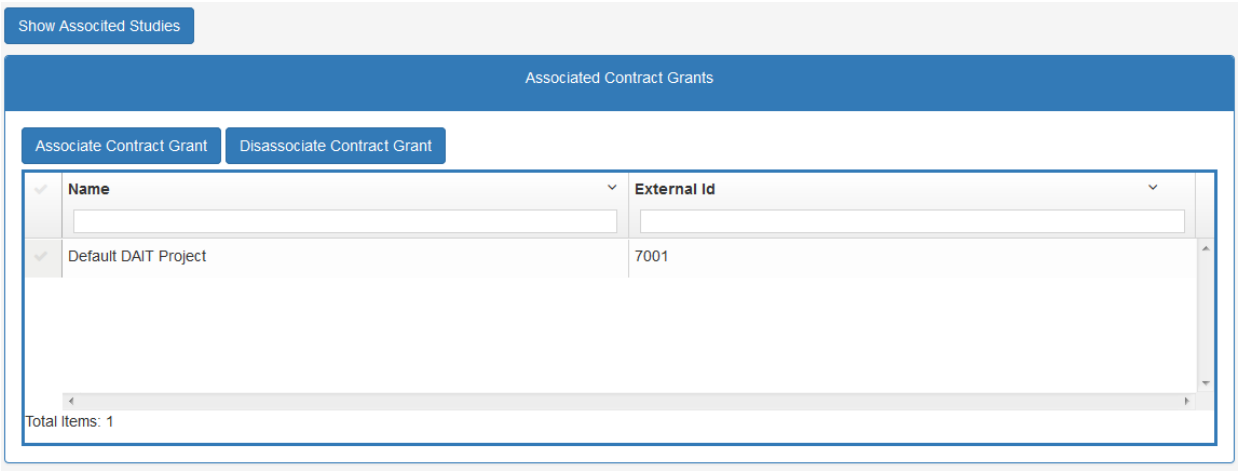
Post- Conditions - The Private Project Workspace details are displayed of the selected Private Project Workspace Project.

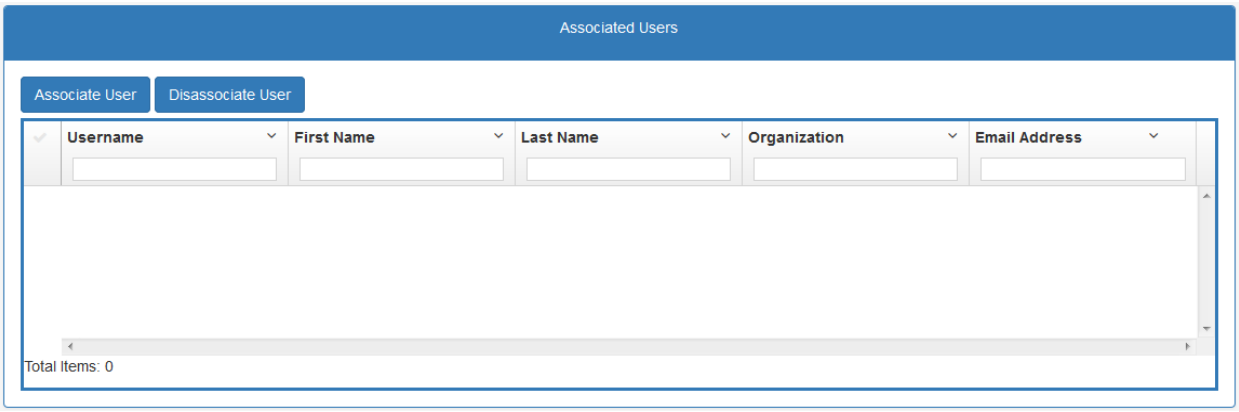
Steps:

1. A "**Private Project Workspace Details**" screen is displayed.

1.2.1.15 Update Workspace







Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Title	Textbox	Y	Y		Text	RESEARCH_PROJECT_INFO	TITLE
Category	Dropdown	Y	Y		Text	RESEARCH_PROJECT_INFO	PROJECT_CATEGORY
Description	Textbox	Y	Y		Text	RESEARCH_PROJECT_INFO	DESCRIPTION
Contract-Grant	Multi-select	NA	Y			RESEARCH_PROJECT_INFO	CG_ID
Associated Users	Label					PROJECT_ASSIGNED_USER	
Name	List Item	NA	N		Text	USER_INFO	FIRST_NAME, LAST_NAME
Phone	List Item	NA	N		Text	USER_INFO	PHONE_NUMBER
Organization	List Item	NA	N		Text	USER_INFO	INSTITUTION
Email	List Item	NA	N		Text	USER_INFO	EMAIL_ADDRESS
Add							
Remove							

The use case describes the process of updating Private Project Workspace screen.

Actor: A user with the BISCAdministrator Role

Pre-Conditions - The user has clicked the Update Private Project Workspace button on the "Search Private Project Workspace" screen.

Post- Conditions - The Private Project Workspace details are updated in the database
Steps:

1. The user modifies the data on the "**Update Private Project Workspace**" screen.
2. The user clicks on the Update Research Project button.
3. The user can associate the Research Project to new users.
4. The System updates the associations in the database.

Business Rules:

1.2.1.16 View My Workspace

Field Name	Field Type	Required	Editable	Business Rules/Preferred Values	Data Type	Database Table	Database Column
Select Box	Option Button						
Title	Textbox	NA	N		Text	RESEARCH_PROJECT_INFO	TITLE
Category	Dropdown	NA	N		Text	RESEARCH_PROJECT_INFO	PROJECT_CATEGORY
Description	Dropdown	NA	N		Text	RESEARCH_PROJECT_INFO	DESCRIPTION
View Private Project Workspace Details							

The use case describes the screens that display the Research Projects of the logged in user.

Actor: A user with the **ImmportDAITUser or the ImmportSharedDataUser role**

Pre-Conditions: The user has logged in to the Immport3.
Post- Conditions - The user views his associated Private Project Workspaces.

Steps:

1. The user clicks on the My Research Projects menu.
2. The "**My Private Project Workspaces**" screen is displayed which lists all the Private Project Workspaces that the user belongs to.
3. The user can click on a Private Project Workspace link and the "Private Project Workspace Details" screen is displayed.

1.3 MENUS OPTIONS

Menu	Roles
Update Profile-Self	**BISCAdministrator, ImmportSharedDataUser, ImmportDataProviderUser**
Change Password-Self	**BISCAdministrator, ImmportSharedDataUser, ImmportDataProviderUser**
Create Program	**BISCAdministrator**
Search/Update Program	**BISCAdministrator**
Create Contract-Grant	**BISCAdministrator**
Search/Update Contract-Grant	**BISCAdministrator**
Create Private Project Workspace	**BISCAdministrator**
Search/Update Private Project Workspace	**BISCAdministrator**
My Private Project Workspaces	**BISCAdministrator, ImmportSharedDataUser, ImmportDataProviderUser**