PentaISF™

Security

User Manual
V3.2

Table of Contents

1. Approval Limit

1.1. Description

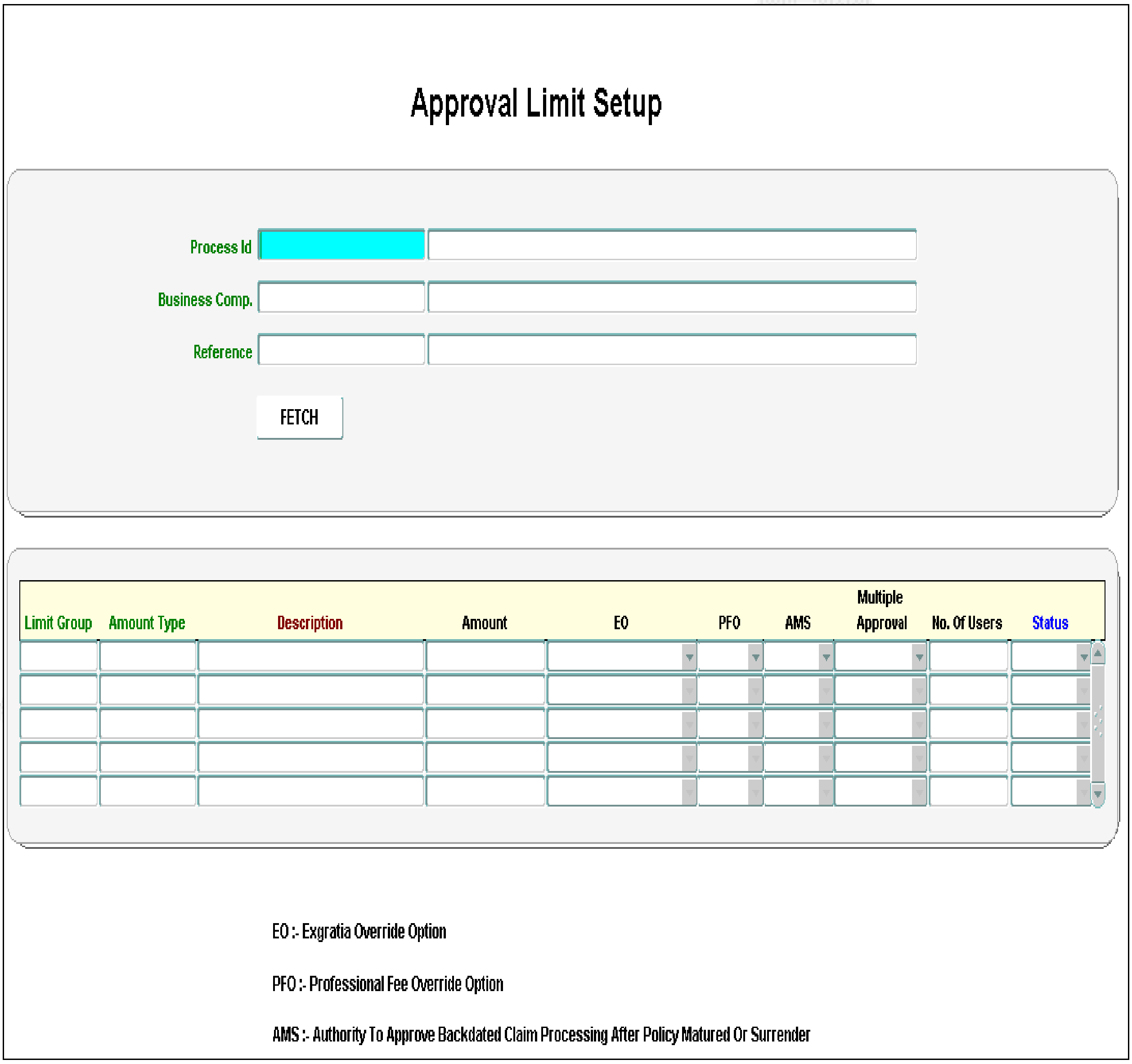
This process is initiated setup the approval limit.

Big Picture:

Enter Approval Limit Details

1.2. Follow Steps

1. Go to **Security** menu, select **Approval Limit**, the screen will be displayed.



☞	**Tips** If you are setting an **Approval Limit** for the entire process, you need not enter **Business Component** and **Reference** details.

☞	**Tips** When you see  in the status bar, you can press **F9** to see the list of values.

2. Enter **Process Id.**
3. Enter **Business Comp.**
4. Enter **Reference.**
5. Enter **Limit Group**.
6. Enter **Amount Type**.
7. Enter **Amount.**
8. Select **EO** whether it is **Not Applicable, Above 100%** or **Below 100%.**
9. Select **PFO** whether **Yes** or **No.**
10. Select **AMS** whether **Yes** or **No.**
11. Select whether **Multiple Approval** is required.
12. Enter **No. of Users**.
13. Select **Status** of the approval limit, whether it is Active or Inactive.
14. Click **Save** button to save your information.
15. Click **Exit** button to exit.

1.3. Screen Glossary

Fields	Description
Process Id	Process identification for which the approval limit will be set for.
Business Comp	Business component of the process code.
Reference	A reference of the particular business component value.
Limit Group	A unique code for limit group.
Amount Type	Amount type, i.e. Sum Covered amount, Surrender value etc.
Description	Description of the amount.
Amount	Amount.
EO	To indicate the ex-gratia over ride option is applicable, above 100% or below 100%.
PFO	Professional Overriding Option. Yes – Allow user to override the default payment up to maximum limit. No – Does not allow user to change the default amount.
AMS	Authority to approve backdated claim process after contract matured and surrendered. Yes – Allow user to approve the claim.
Multiple Approval	Indicates whether multiple approvals is required.
No. of Users	If Multiple Approval is No, number of user for approval will be 1. If Multiple Approval is Yes, enter the number of users required for approval.
Status	Indicates whether the record is active or not.

1.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

2. Amount Type

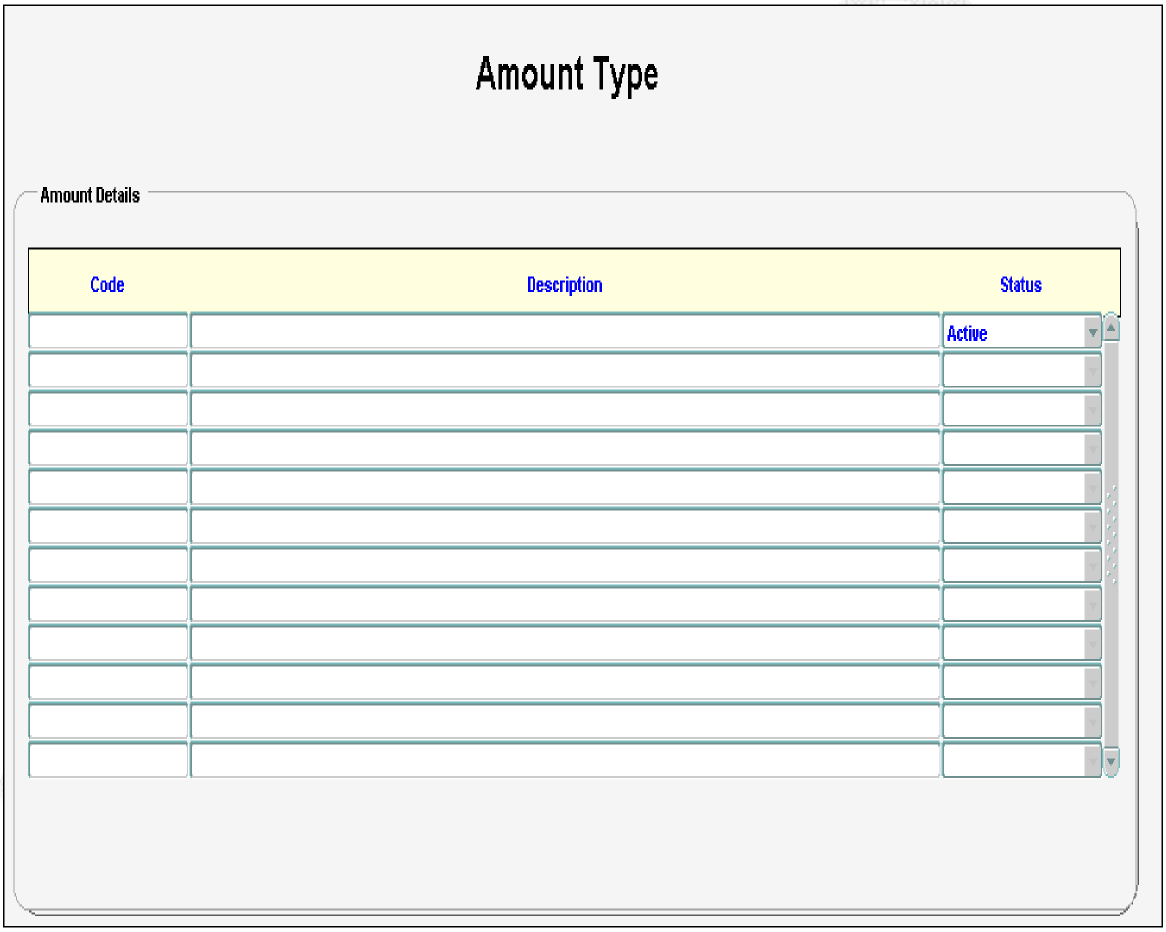
2.1. Description

This process is initiated to setup the amount type.

Big Picture:

2.2. Follow Steps

1. Go to **Security** menu, select **Security → Amount Type**, the screen will be displayed.



2. Enter **Amount Type Code**.
3. Enter **Amount Type Description**.
4. Select **Status** of the record, whether it is **Active** or **Inactive**.
5. Click **Save** button to save your information.
6. Click **Exit** button to exit.

2.3. Screen Glossary

Fields	Description
Amount Type Code	A unique code used to identify a particular type of amount.
Amount Type Description	A description of the type of amount, i.e. Surrender Value, Loan Amount etc.
Status	Status of the record, whether it is Active or Inactive.

2.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

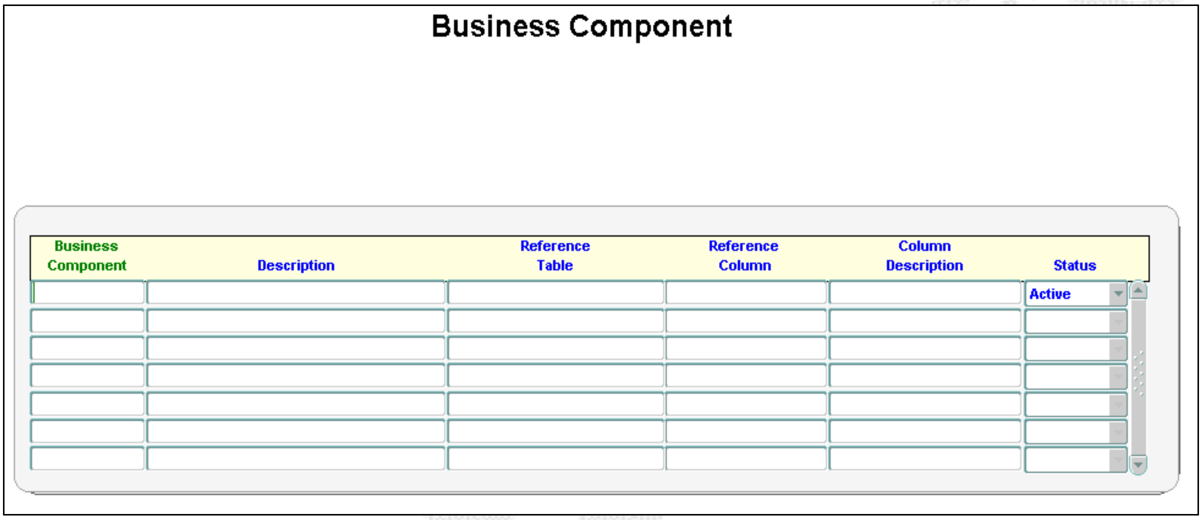
3. Business Components

3.1. Description

This process is initiated to setup business components.

3.2. Follow Steps

1. Go to **Security** menu, select **Security → Business Components**, the screen will be displayed.



☞	**Tips** To query existing business components, press **F9** key, select an existing value and click **OK** button. The business component information will be displayed.

2. Enter **Business Component**. **Description** will be populated.
3. Enter **Reference Table.**
4. Enter **Reference Column**.
5. Enter **Column Description**.
6. Click **Save** button to save your information.
7. Click **Exit** button to exit.

3.3. Screen Glossary

Fields	Description
Business Component	A code used to identify a particular business component.
Description	A description of the business component.
Reference Table	Array of values for the business component will be available in the Reference Table.
Reference Column	Reference column code used for the business component value.
Column Description	A description of the reference column.
Status	Status of the record.

3.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

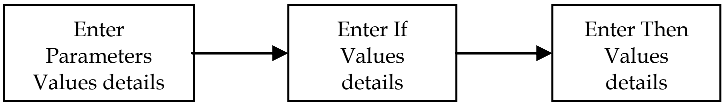
4. Security Masters (General Parameters)

4.1. Description

This master setup contains Security General Parameters.

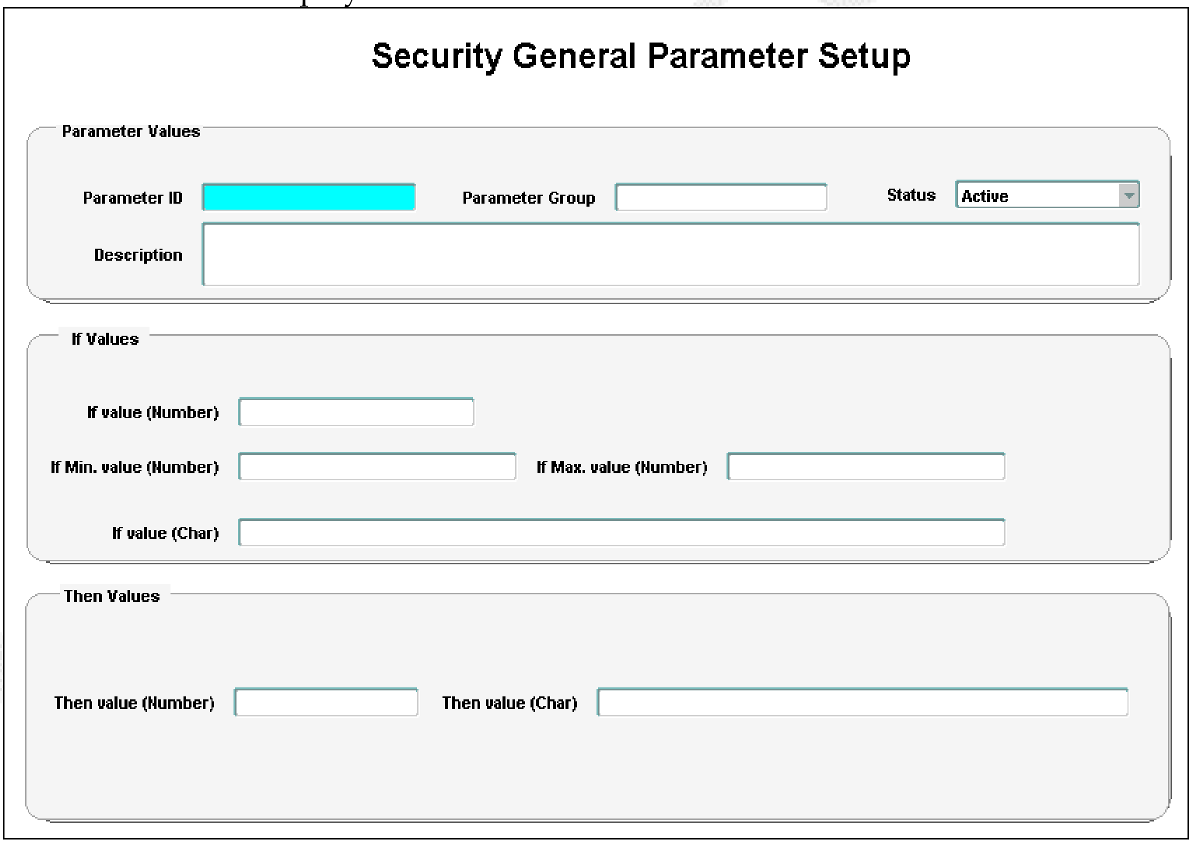
Status: Frozen.

Big Picture:



4.2. Follow Steps

1. Go to the **Masters** menu, select **Security → Security Masters →General Parameters**, the screen will be displayed.



2. Enter **Parameters Value** details.
3. Enter **If Values** details.
4. Enter **Then Values** details.
5. Click **Save** button to save your information.
6. Click **Exit** button to exit to main menu screen.

4.3. Screen Glossary

Fields	Description
General Parameters	
Parameter Values	
Parameter ID	A unique code/ name used to identify the particular parameter identification.
Group	Parameter group.
Status	Status of the record, whether it is active or inactive
Description	A description of the parameter, i.e. The capital amount used in illustration report.
If Values	
If value (Number)	Values defined.
If Min. value (Number)	Values defined.
If Max. value (Number)	Values defined.
If value (Char)	Values defined.
Then Values	
Then value (Number)	Values defined.
Then value (Char)	Values defined.

4.4. Error Message

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

5. Security Masters (User Profile Administration)

5.1. Description

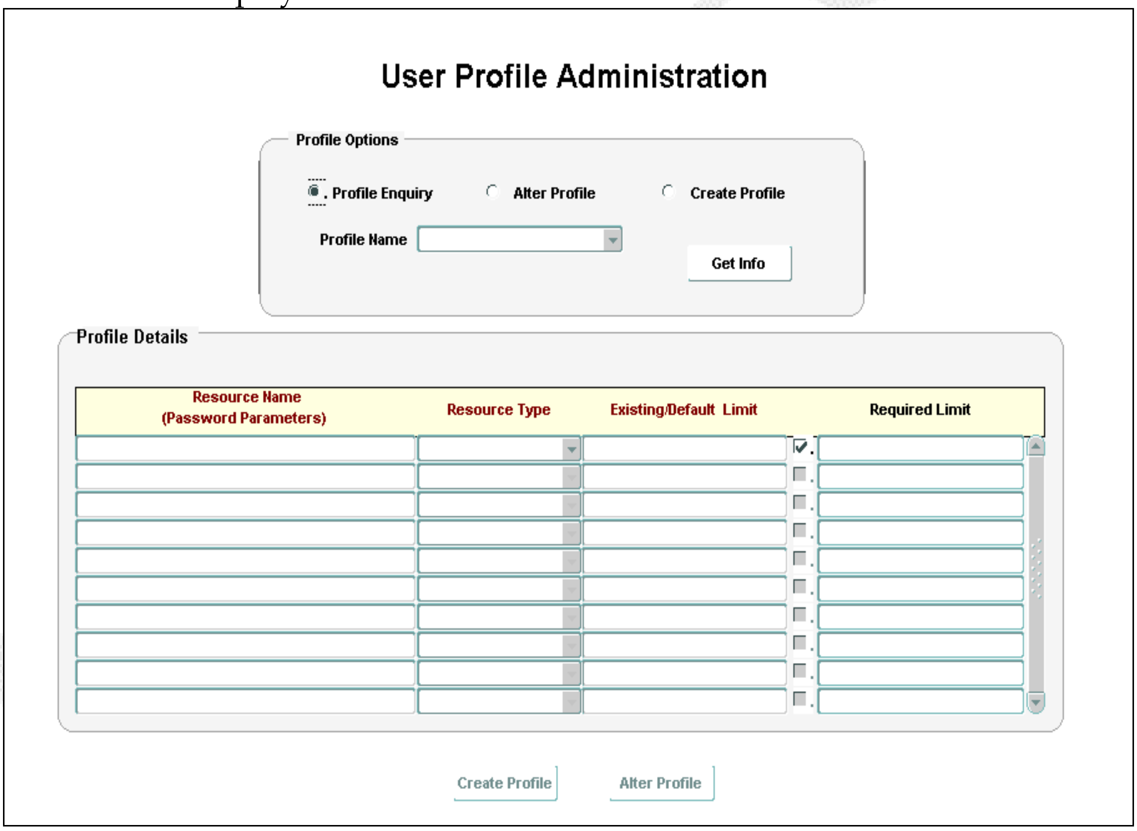
This master setup contains Security User Profile Administration to query, create or alter a profile.

Status: Frozen.

Big Picture:

5.2. Follow Steps

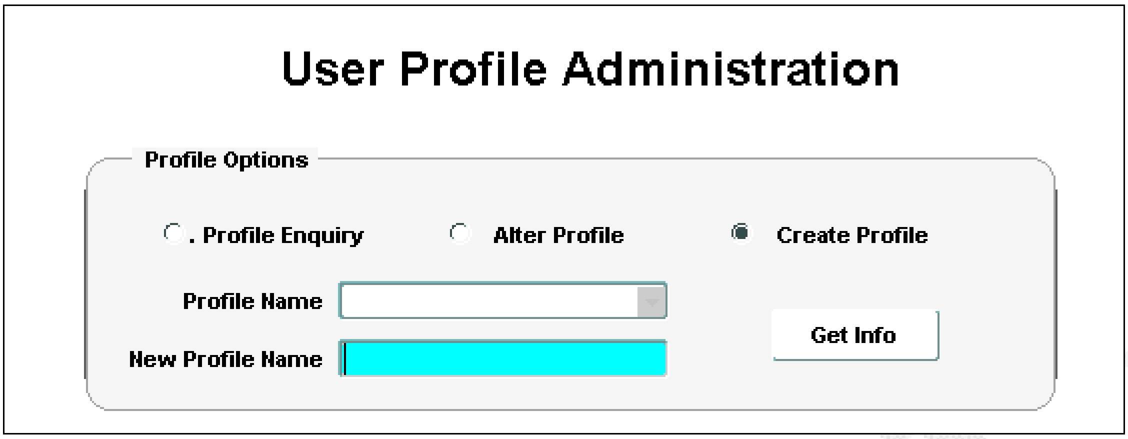
1. Go to the **Security** menu, select **Security Masters** →**User Profile Administration**, the screen will be displayed.



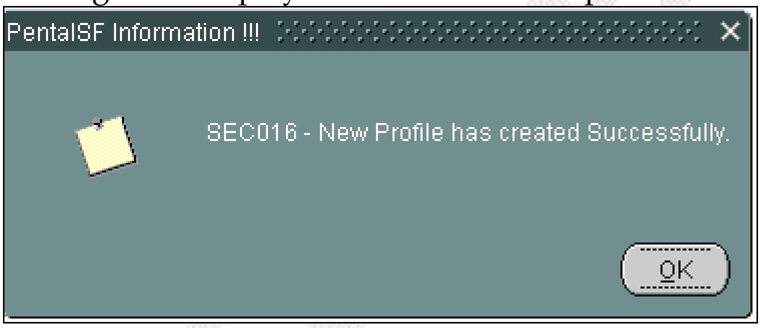
2.Enter **Profile Options** either Profile Enquiry/Alter Profile/ Create Profile.
3.If user has selected **Profile Enquiry** radio button, proceed to select the **Profile Name**.
4.Click 

button to display the information from filter option.
5.Place a tick at the checkbox.
6.Enter **Required Limit**.

7. If user has selected the **Create Profile Radio button**, the Create button will be enabled now.

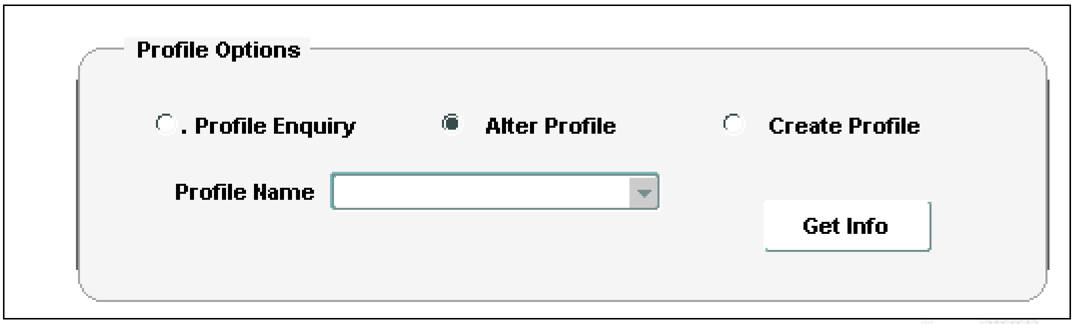


- Enter **New Profile Name**.
- Click Get Info button to display the information from filter option.
- Place a tick at the checkbox.
- Enter **Required Limit.**
- Click Create Profile button to create the new profile.
- Message will display to confirm the new profile creation.

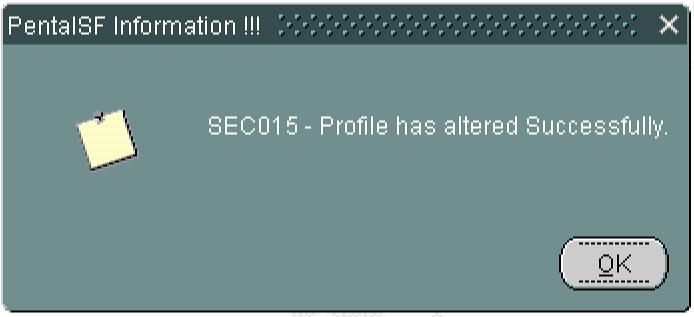


Click OK button to acknowledge.

8.If user has selected the **Alter Profile Radio button**, the Alter button will be enabled now.



- Select **Profile Name**.
- Click  button to display the information from filter option.
- Place a tick at the checkbox.
- Enter **Required Limit.**
- User can click the  button to alter the profile.
- Message will display to confirm the altered profile.



Click OK button to acknowledge.

9.Click **Exit** button to exit to main menu screen.

5.3. Screen Glossary

Fields	Description
Profile Options	
Profile Enquiry Radio button	Click this radio button to perform a profile query.
Alter Profile Radio button	Click this radio button to alter a profile.
Create Profile Radio button	Click this radio button to create a profile.
Profile Name	Indicate the Profile Name as Default Profile or a Monitoring Profile.
New Profile Name	This filed appears when user clicks Create Profile radio button. User must enter the new profile name.
Get Info button	Click this button to retrieve the requested information based on the filter profile options.
Profile Details	
Resource Name(Password Parameters)	Shows the resource name (password parameters details). For example: Failed Login Attempts, Password Life Time, Password Lock Time, Password Verify Functions, etc.
Resource Type	Shows resource type as password or kernel.
Existing/Default Limit	Shows the allowable existing limits allocated to users by administrator.
Check box	Place a tick at the check box to create, alter or make profile queries.
Required Limit	Shows the required limit set by the administrator for the users.
Alter button	Click this button to alter a profile.
Create button	Click this button to create a profile.

5.4. Error Message

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

6. Security Masters (Security Matrix)

6.1. Description

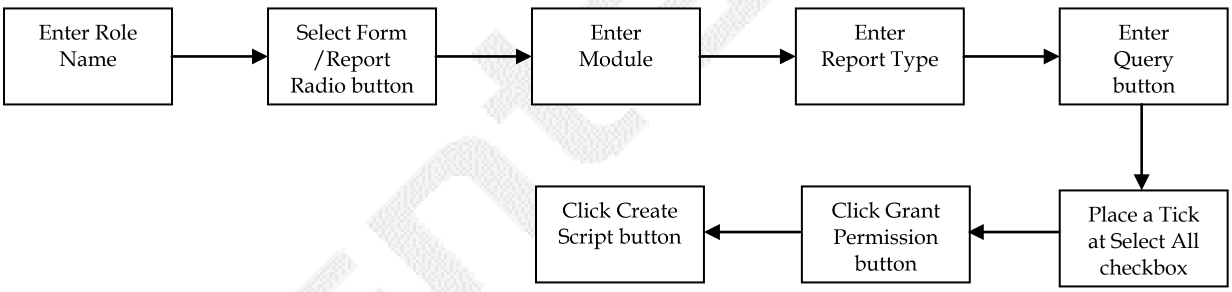
This master setup contains the access reports through ROLES, same as in accessing of forms. DBA and/or administrator will have to create separate roles and assign respective reports to those roles. Roles are create for each module (i.e. Agency, NB, Finance etc), but it is not compulsory to do so.
Like in forms, hereafter you can assign individual reports to users as well.
Once user login into the system, it will show reports only those are assigned to user.

Currently, to give access to the PentaISF Application forms, DBA and/or administrator have to write the scripts manually and run in backend. Using this new security Matrix form, we will be able to stop this. In addition, we have added a feature of report security to our application security module with the aid of security Matrix. Main concept has not changed as all forms & reports are assigned to pre defined Database roles.

Note: Database Administrator must create Roles in the Database.

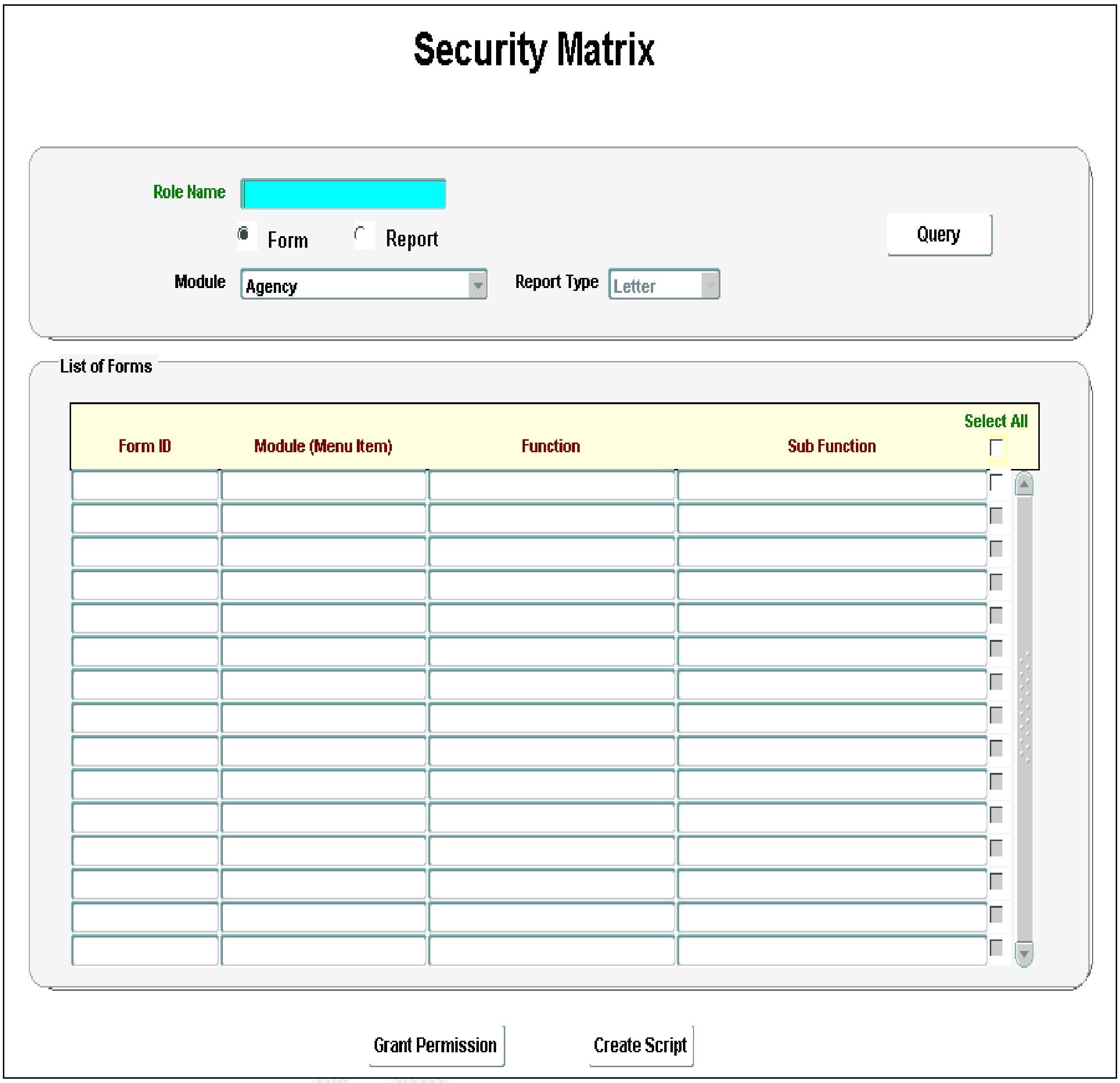
Status: Frozen.

Big Picture:



6.2. Follow Steps

1. Go to the **Security** menu, select **Security Masters →Security Matrix**, the screen will be displayed.



2. Enter **Role Name.**
3. Select **Form or Report** radio buttons. Note: Depending on selection, Module list will be listed.
4. Select **Module.**
5. Select **Report Type**.
6. Click **Query** button.
7. Place tick at **Select All**.
8. Click **Grant Permission** button.
9. Click **Create Script** button.
10. Click **EXIT** icon.

6.3. Screen Glossary

Fields	Description
Security Matrix	
Role Name	Press F9 key to get the list of all database roles. DBA and/or administrator have to decide & create valid roles.
Form or Report radio buttons	User has to choose either form or report option. • If user selects Form option, list of modules will be populated to Module field and report type field will be disabled. • If user selects report option, list of modules related to reports will be populated to Module field and Report Type will be enabled with relevant list values. Lower block of the form will display different data based on user's selection of this option.
Module	Displays the list of modules.
Report Type	Displays the report type.
Query button	Once user presses the query button, all details of either forms or reports will be populated into the lower block. • If user select forms option it will display, Form ID, Module, Function & sub-function details. • If he selects reports it will show report ID, Module, Report type & report description.
List of Forms	
Form ID	Indicate the Form Identification like AM_FRM_12, NB_FRM_01,etc.
Module (Menu)	Name of the menu item like New Business, Re-Takaful, etc.
Function	Indicate the function of the module or menu items like Masters.
Sub Function	Indicates the sub function of the module or menu item like Training Master for Agency function.
Select All	Place a tick in the check box to indicate which form or report that requires to be generated. User has the option to select all forms in one time. User has the choice to use this "select all" option or to choose selected objects by ticking individual check boxes.
Grant Permission Button	This will grant the access of all selected form and/or reports to the particular role.
Create Script button	Once user press this it will open up a file saving dialogue box which shows the file path & file name of the script to be generated. Once it has generated DBA and/or administrator has to run the script manually.

6.4. Error Message

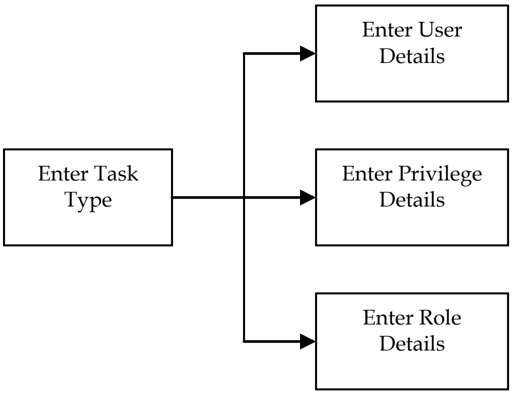
No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

7. Security Administration (Help Desk)

7.1. Description

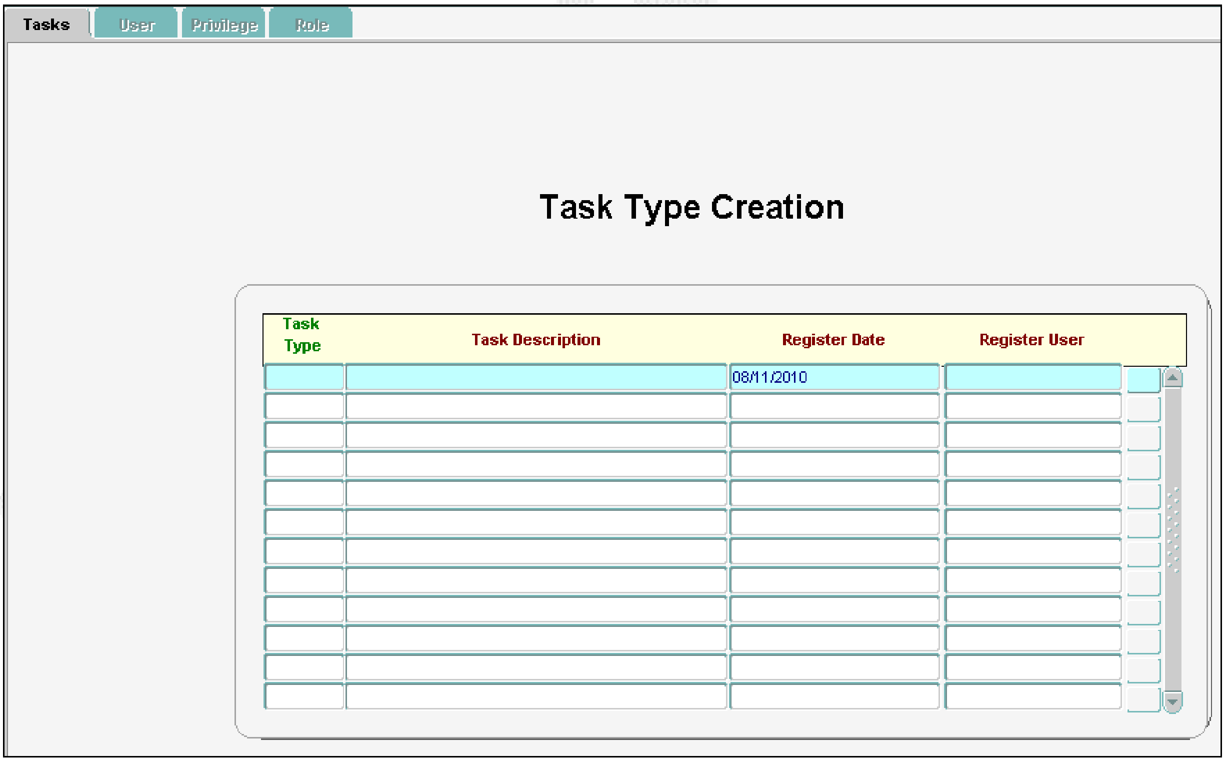
This process is initiated by the help desk to create tasks.
The approval will be done by the security administrator.

Big Picture:

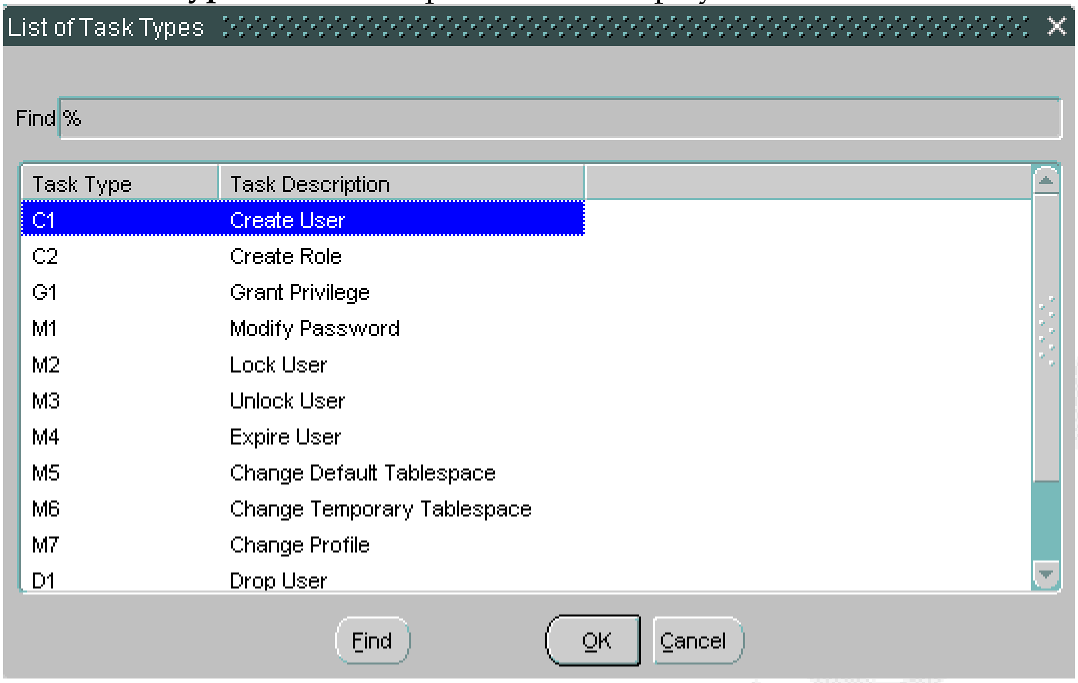


7.2. Follow Steps

1. Go to the **Security** menu, select **Security Administration → Help Desk**, the screen will be displayed.

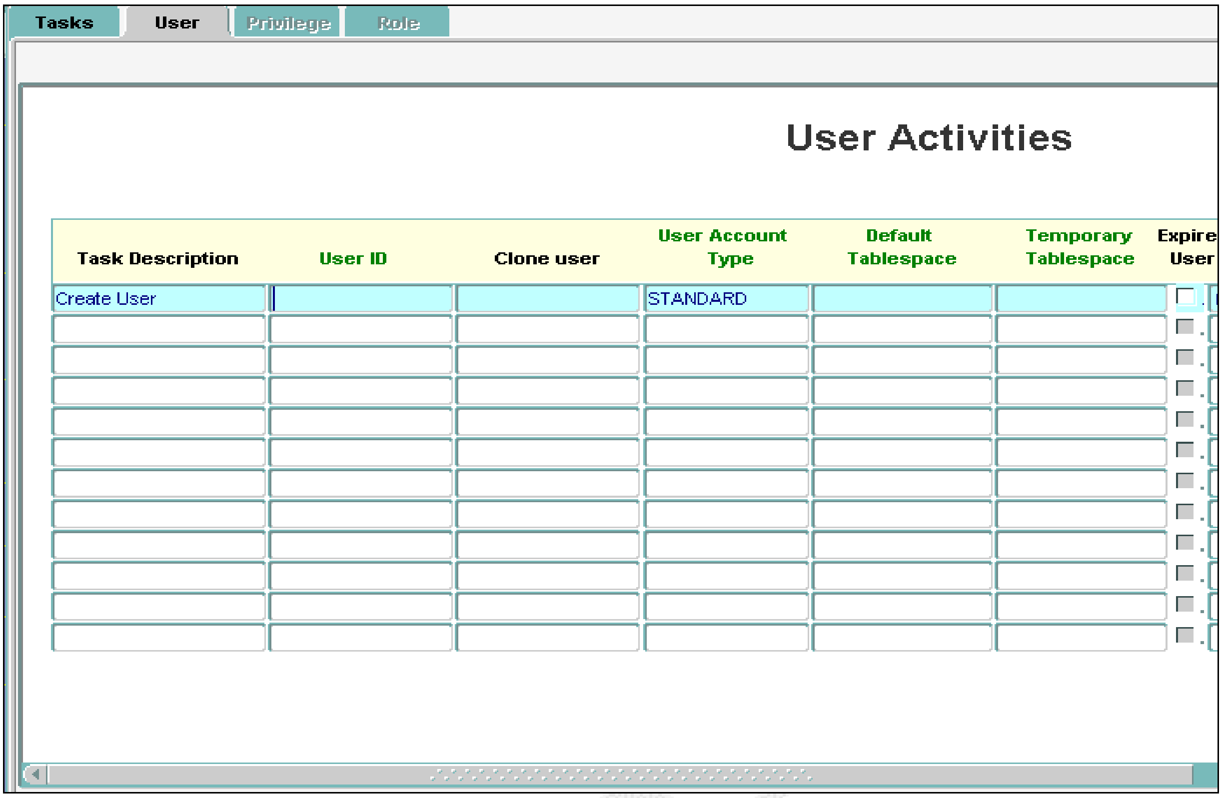


2. Enter **Task Type**. Task description will be displayed.

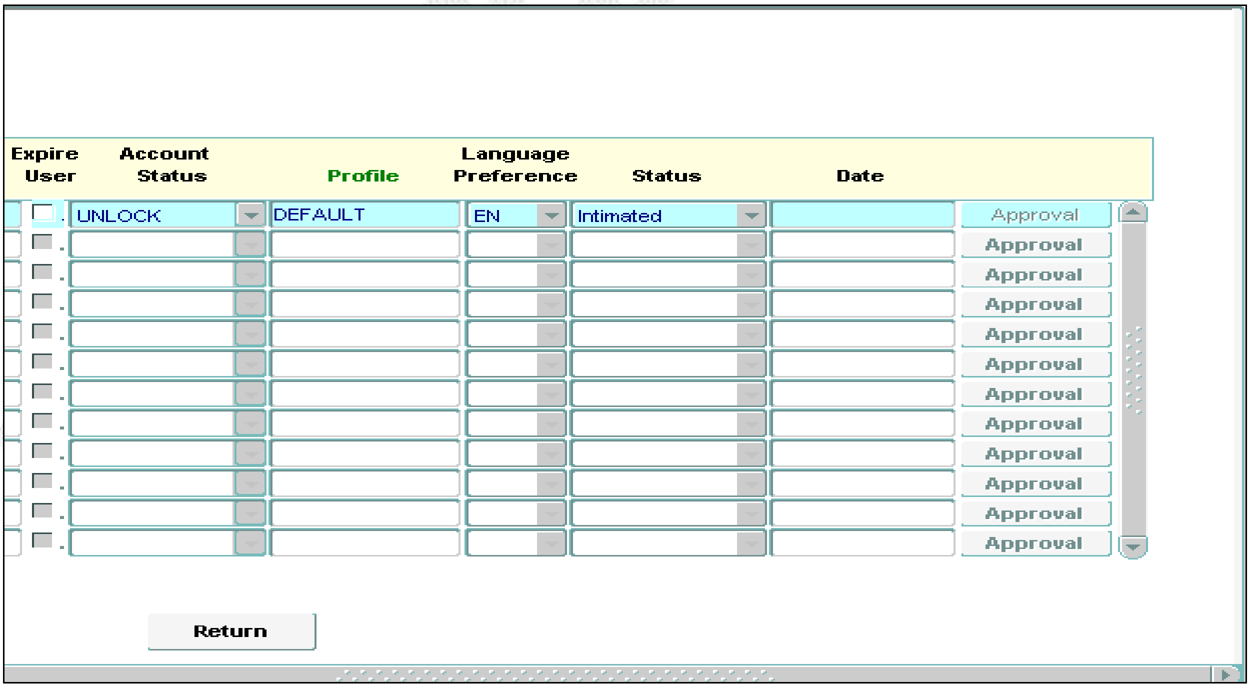


☞	**Tips** • For Task Type C1, M1, M2, M3, M4, M5, M6, M7 and C3, the User Tab will be displayed. • For Task Type C2 and D2, the Role Tab will be displayed. • For Task Type G1 and G2, the Privilege Tab will be displayed.

User Tab



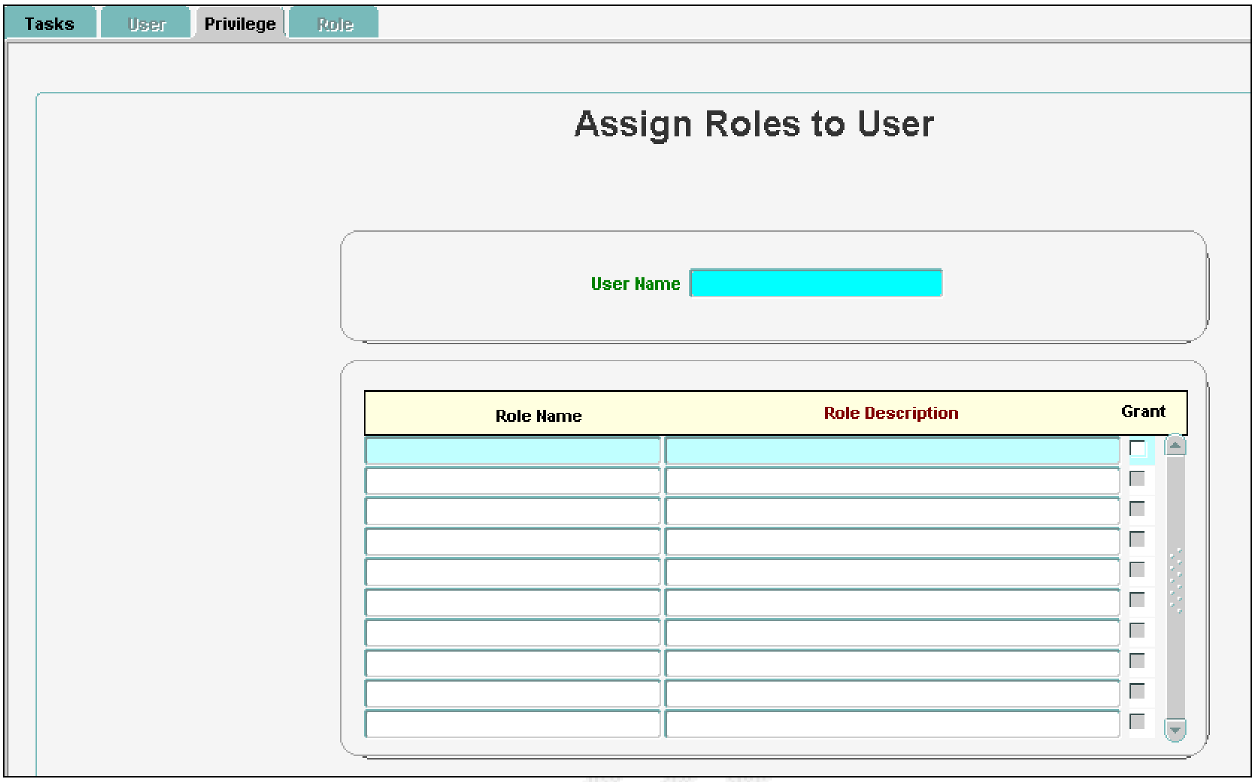
continued…



3. Enter user activities details. Refer to screen glossary for more details.
4. **Register Date** will be defaulted to today's date.

Privilege tab

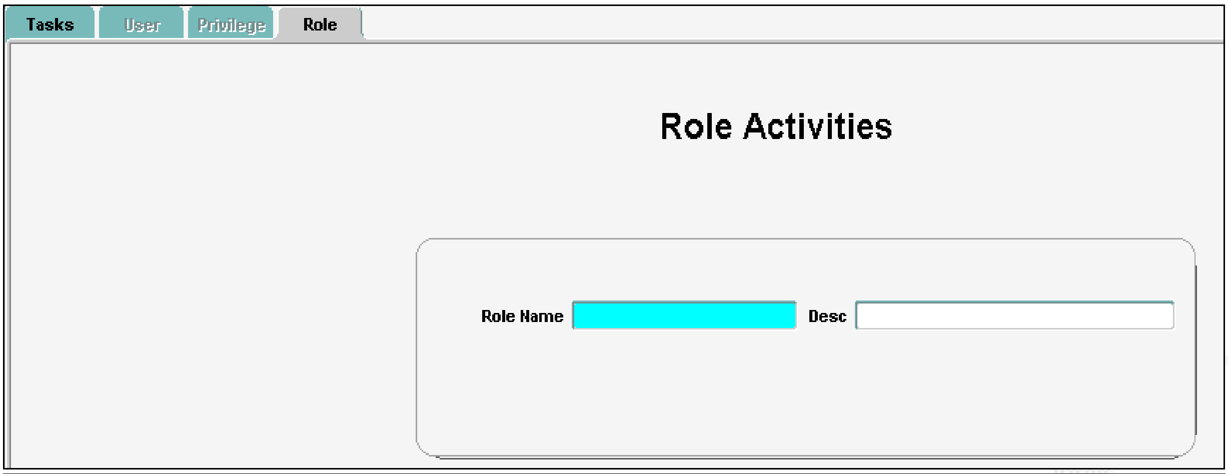
This tab will only be displayed if you are granting privilege to a user.



5. Enter **User Name**.
6. **Grant** role to the user by marking the checkboxes.
7. Revoke role from the user by un-marking the checkboxes.

Role Tab

This tab will only be displayed if you are creating role for the user.



8. Enter **Role Name**.
9. Click **Save** button to save your information.
10. Click **Exit** button to exit.

7.3. Screen Glossary

Fields	Description
Tasks tab	
Task Type	Task code.
Task Description	Type of task to perform, i.e. Create User, Create Role, Grant Privilege etc.
Register Date	Date on which this task is registered.
Register User	Show the registered user.
User tab	
Task Description	Description of the task.
User Name	Login identification for the user.
Clone User	User whose details are to be cloned.
Default Tablespace	To indicate that the objects owned by the user will be created.
Temporary Tablespace	To indicates an area which will be used for doing the temporary operation such as sorting a data or grouping a data.
Expire User	To make the password expired, so that user is required to change the password.
Account Status	**Lock**: To indicate that the user name will be locked if the user enters the password wrongly for 3 times. **Unlock**: To indicate that the user name will not be locked if the user enter the password wrongly for 3 times or more.
Profile	Profile is a security feature which controls the following security options: • IDLE_TIME: how long a user can be idle after connecting to the database • CONNECT_TIME: how long a user can be connected to the database • FAILED_LOGIN_ATTEMPTS: how many failed login attempts are allowed for the user • PASSWORD_LIFE_TIME: how long a password is valid before it is forced to be changed • PASSWORD_REUSE_TIME: how many times gap a password can be reused • PASSWORD_REUSE_MAX: how many times a password can be repeated • PASSPWORD_VERIFY_FUNCTION: how complex the password should be • PASSWORD_LOCK_TIME: duration of account lock time after failed login attempts • PASSWORD_GRACE_TIME: grace time before user should change his password

Language Preference	User's language preference.
Status	Status of the task, i.e. intimated, approved or rejected.
Date	Date of the transaction.
Privilege tab	
User Name	Login identification for the user.
Role Name	Role to be granted.
Grant	If this checkbox is marked, it means the role will be granted upon save.
Role tab	
Role Name	Role name.
Description	Description of the role name.

7.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	The user name already exists.	You have entered an existing use name.	Enter a new user name.

8. Security Administration (Security Administrator)

8.1. Description

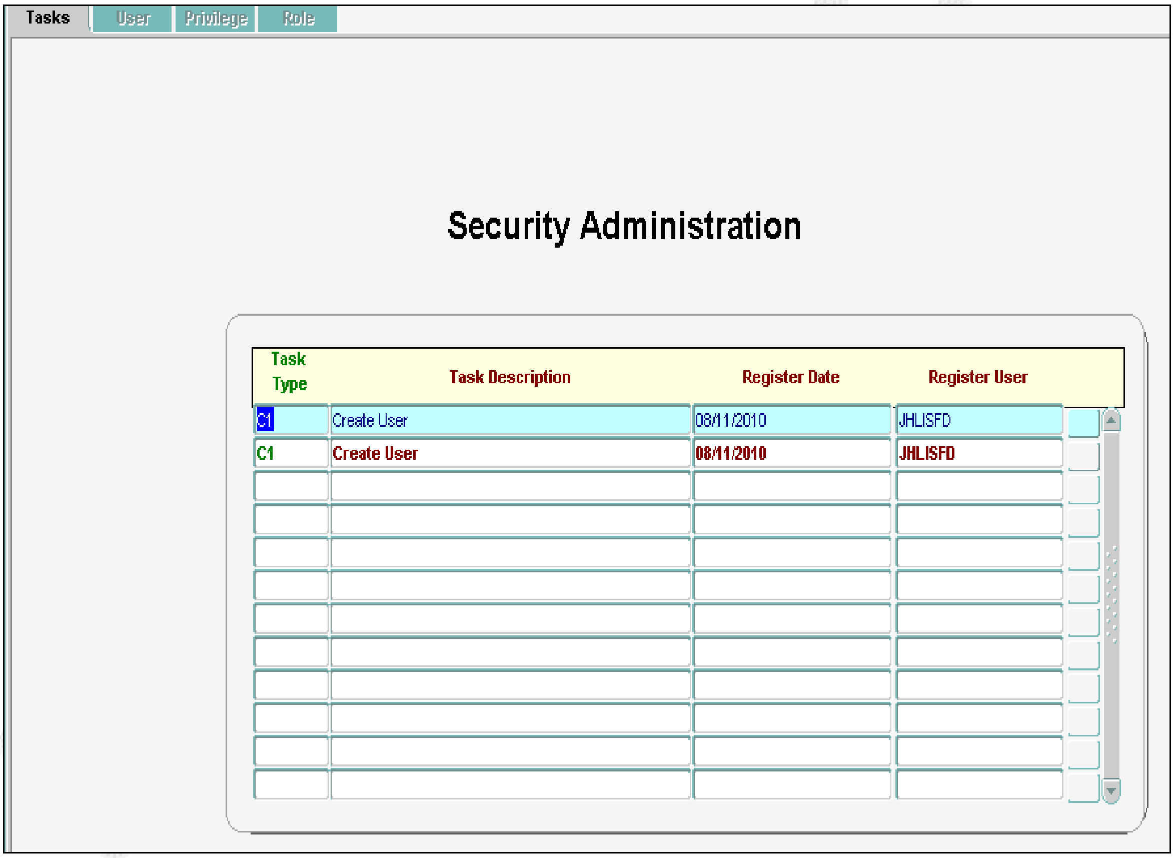
This process is initiated to approve the various task types that were created in the help desk.

Big Picture:

Approve Tasks

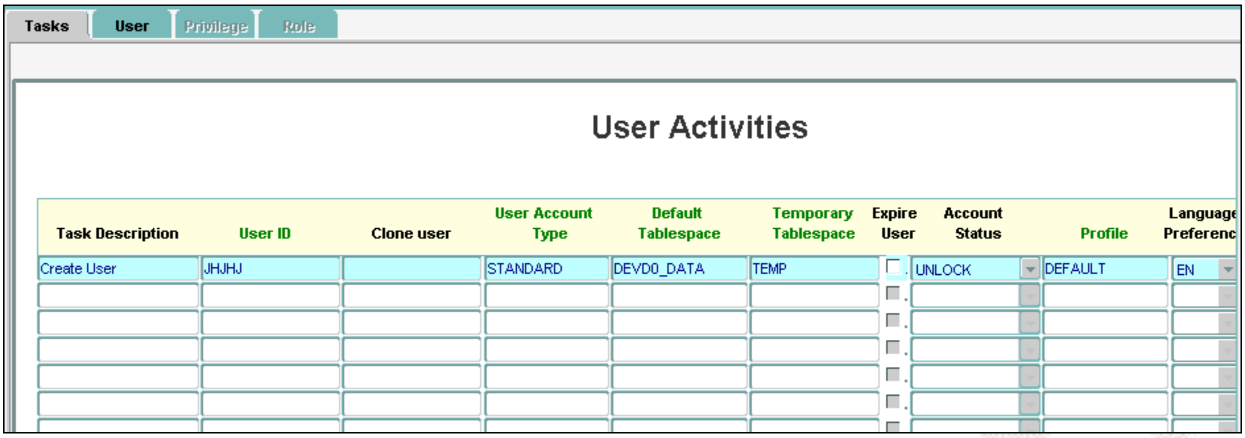
8.2. Follow Steps

1. Go to the **Security** menu, select **Security Administration → Security Administrator**, the screen will be displayed. The tasks that are waiting for approval will be displayed by default.

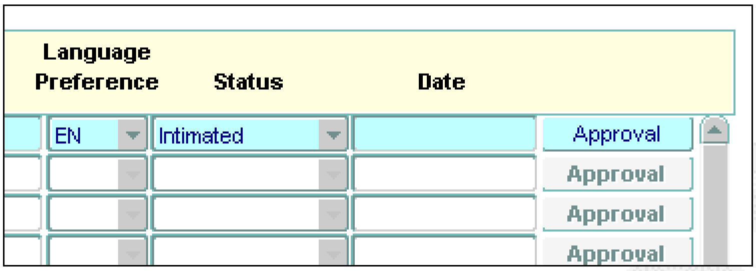


2. Click on the corresponding **Task Type** to go to the corresponding tabs.

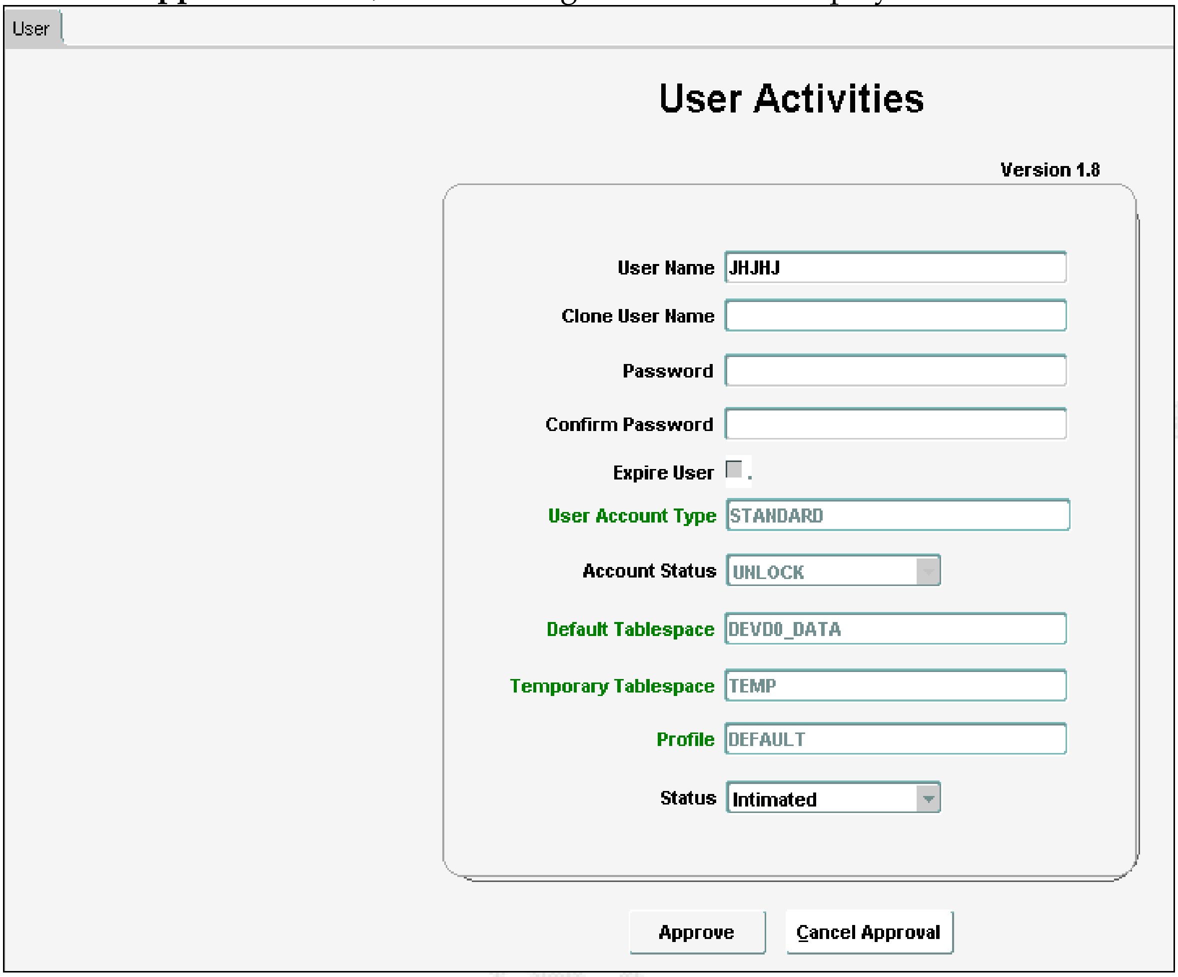
User Task



continue…

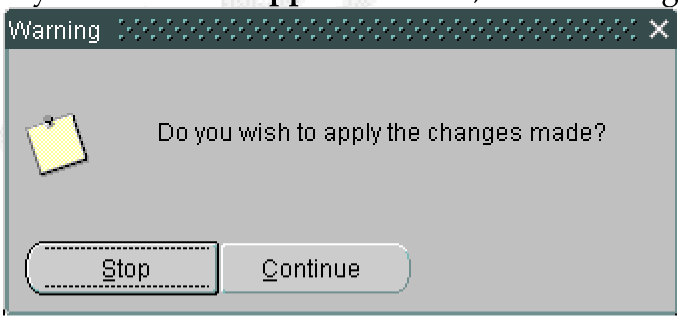


3. Click **Approval** button, the following screen will be displayed.



4. Update the user details.
5. Click **Approve** button to approve.
   Click **Cancel Approval** button to cancel the approval.

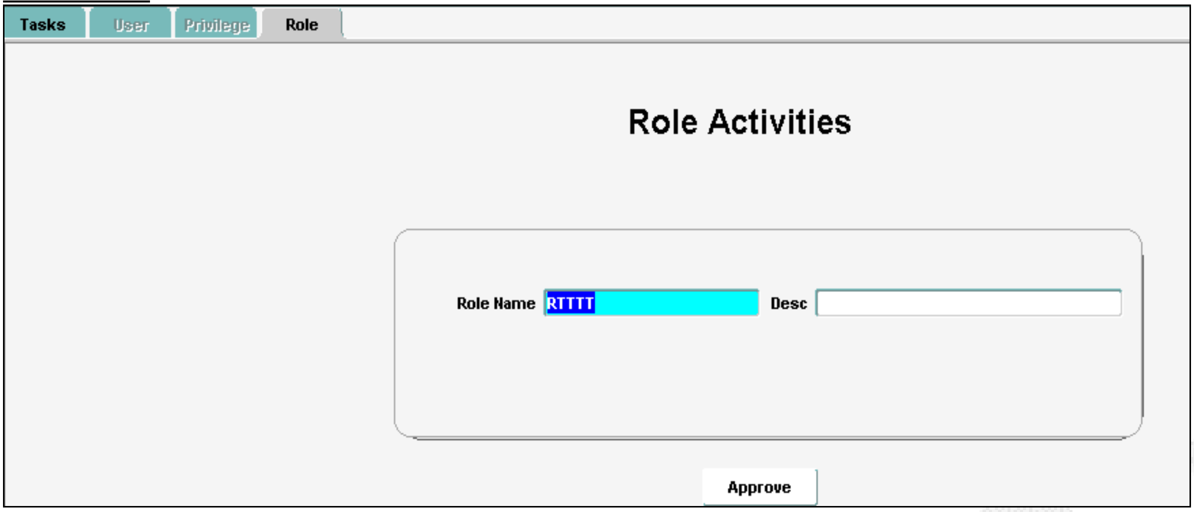
   If you have click **Approve** button, the following will be displayed.



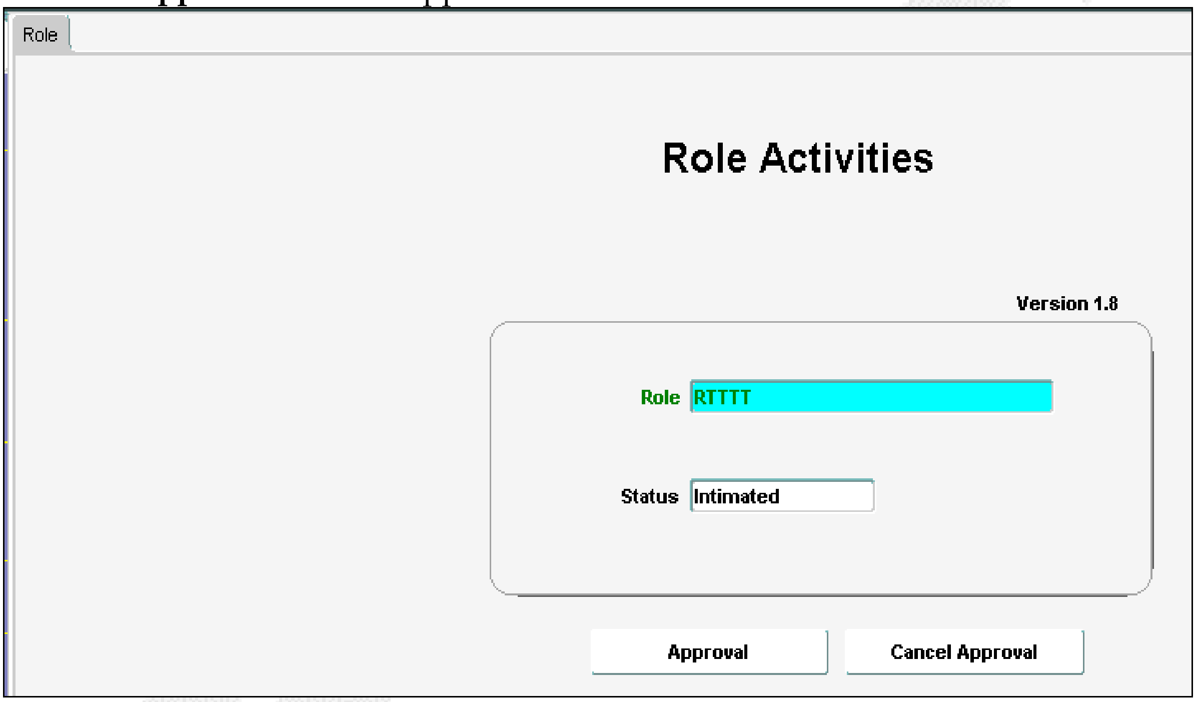
Click **Continue** button to apply the changes made.

Click **OK** button to acknowledge.

Role Task

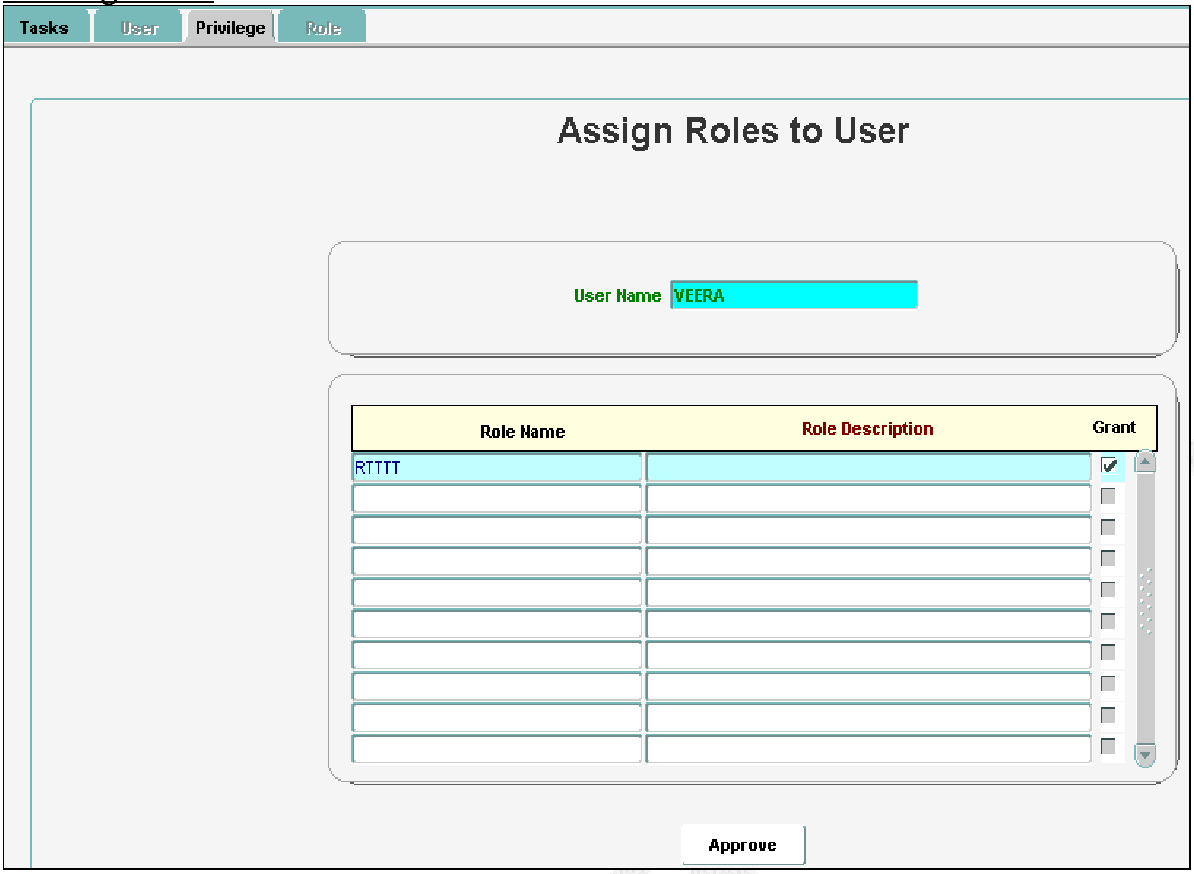


6. Click **Approve** button to approve the role.

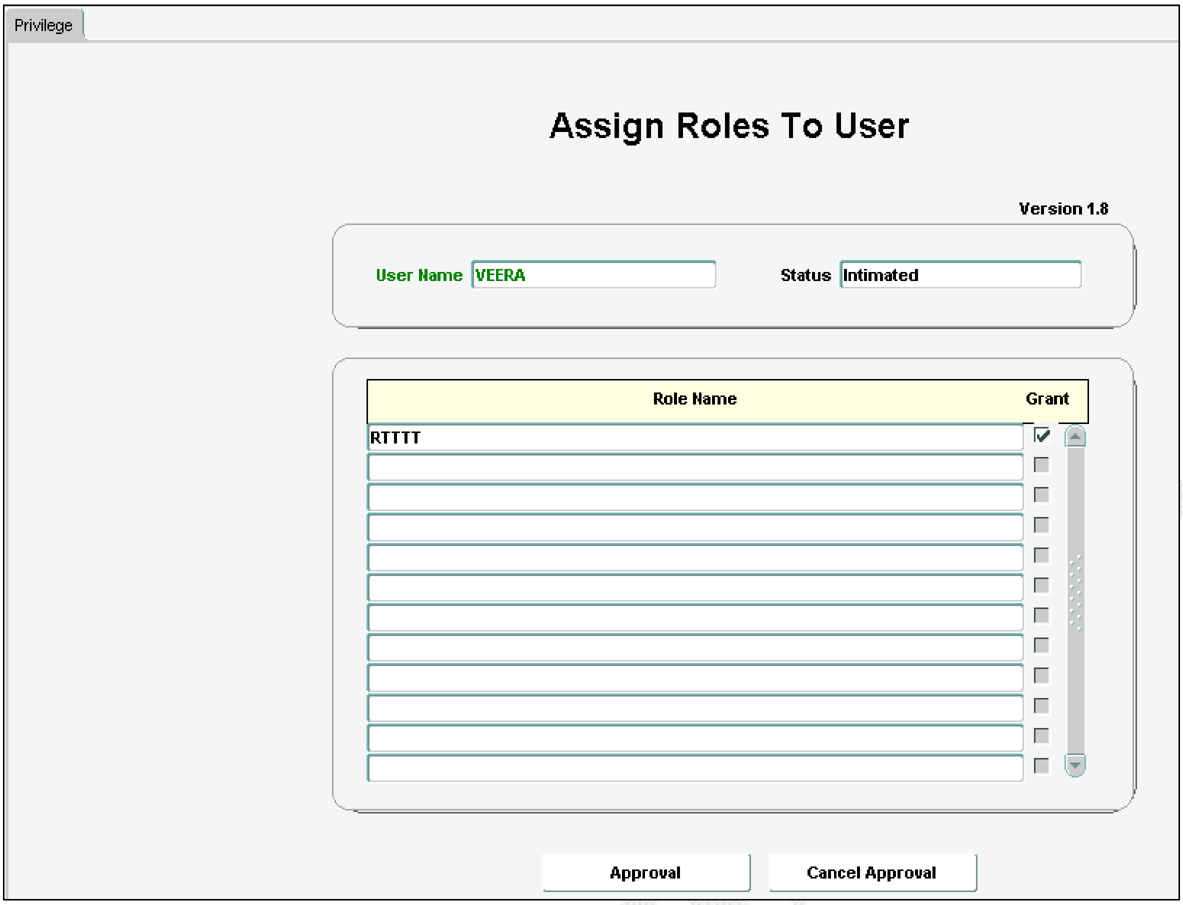


7. Status will be shown as Intimated.
8. Click **Approval** button to approve.
9. Click **Cancel Approval** button to cancel.

Privilege Task



10. Click **Approve** button to approve.



11. Click **Approval** button to approve.
12. Click **Cancel Approval** button to cancel.
13. Click **Exit** button to exit.

8.3. Screen Glossary

Fields	Description
Refer to Security Administration (Help Desk) for more details.	

8.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	Select a Default Tablespace.	You have not selected a default tablespace.	Select a valid default tablespace.
2.	Password & confirm password does not match.	Your new password and confirm password is different.	Retype again to ensure the new password and confirm password is the same.

9. Security Administration (Assign Program to Role)

9.1. Description

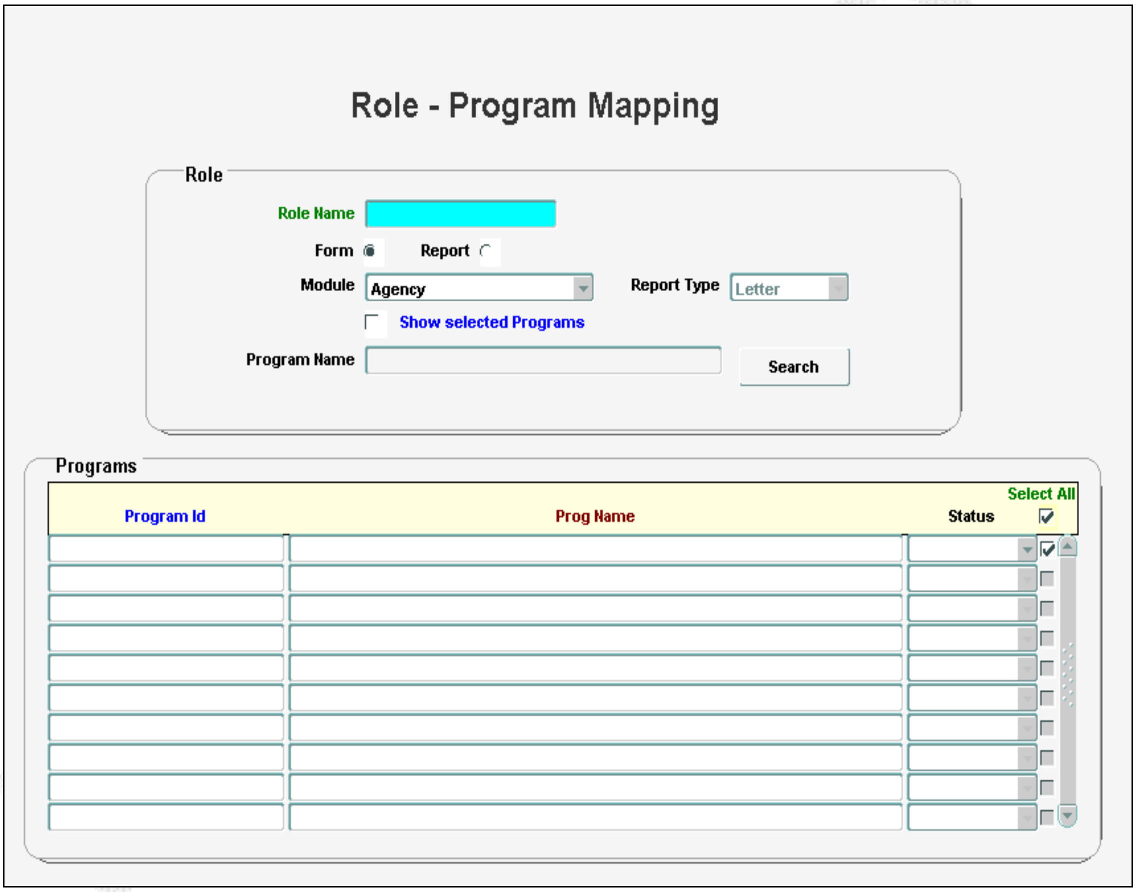
This process is initiated to assign programs to a role, users with the assigned role will be able to access the programs.

Big Picture:

Assign Program to Role

9.2. Follow Steps

1. Go to the **Security** menu, select **Security Administration → Assign Program to Role**, the screen will be displayed.



2. Enter **Role Name**.
3. Assign program to role.
   - Enter **Program Id**
   - Select **Status** of the record.
   - Mark the checkbox to assign the program to the role.
4. Click **Save** button to save your information.
5. Click **Exit** button to exit.

9.3. Screen Glossary

Fields	Description
Role Name	Role name.
Program Id	Program Id.
Program Name	Program description.
Status	Status of the record.
Select All	Indicates whether to assign this program to this role.

9.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

10. Security Administration (Assign Program to User)

10.1. Description

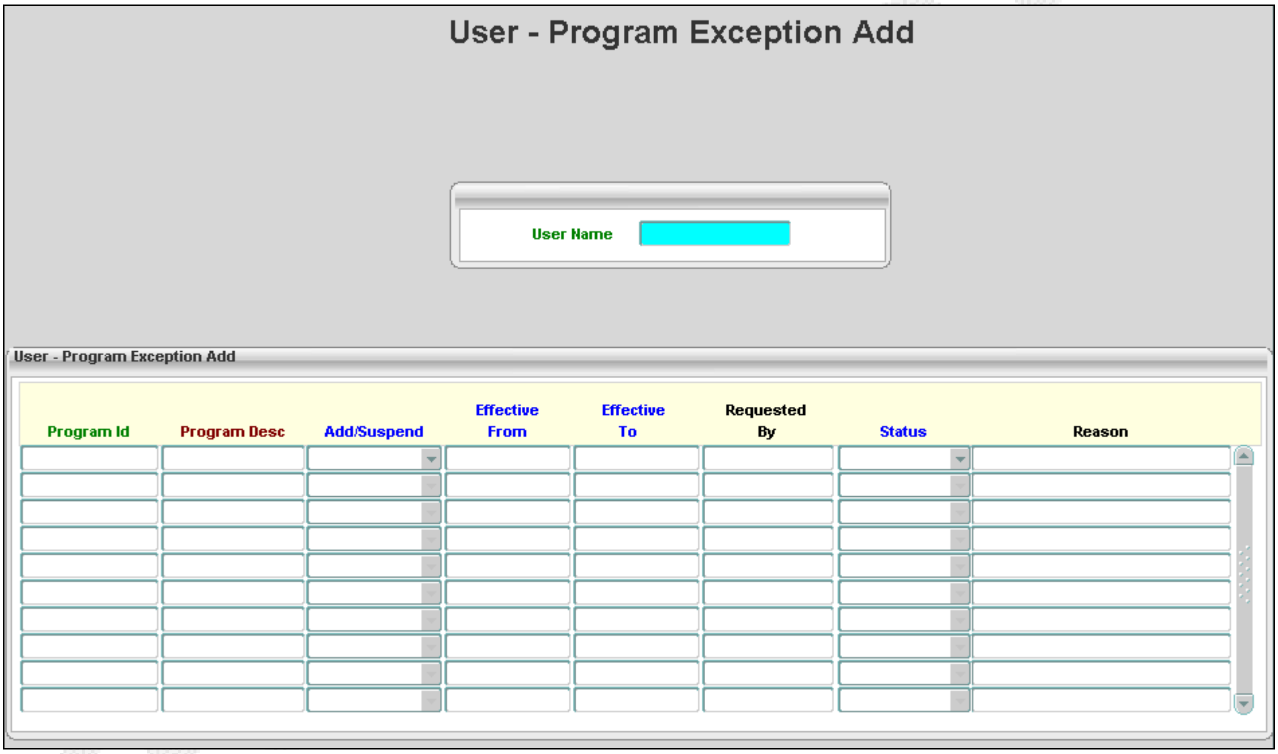
This process is initiated to assign programs to a user.

Big Picture:

Assign Program to User

10.2. Follow Steps

1 Go to the **Security** menu, select **Security Administration → Assign Program to User**, the screen will be displayed.



2. Enter **User Name**.
3. Assign programs to user.
   - Enter **Program Id**
   - Select whether **Add or Suspend** this program to the user.
   - Enter **Effective (From/ To)** date.
   - Enter **Requested By**.
   - Select **Status** of the record.
   - Enter **Reason** if any.
4. Click **Save** button to save your information.
5. Click **Exit** button to exit.

10.3. Screen Glossary

Fields	Description
User Name	User name.
Program Id	Program Id.
Program Desc	Program description.
Add/ Suspend	Indicates whether to add program or suspend program for this user.
Effective (From/ To)	Effective date range of the assignment.
Requested By	Assignment requested by.
Status	Status of the record.
Reason	Reason to add or suspend this program to this user.

10.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

11.Security Administration (Revoke Program From Role)

11.1. Description

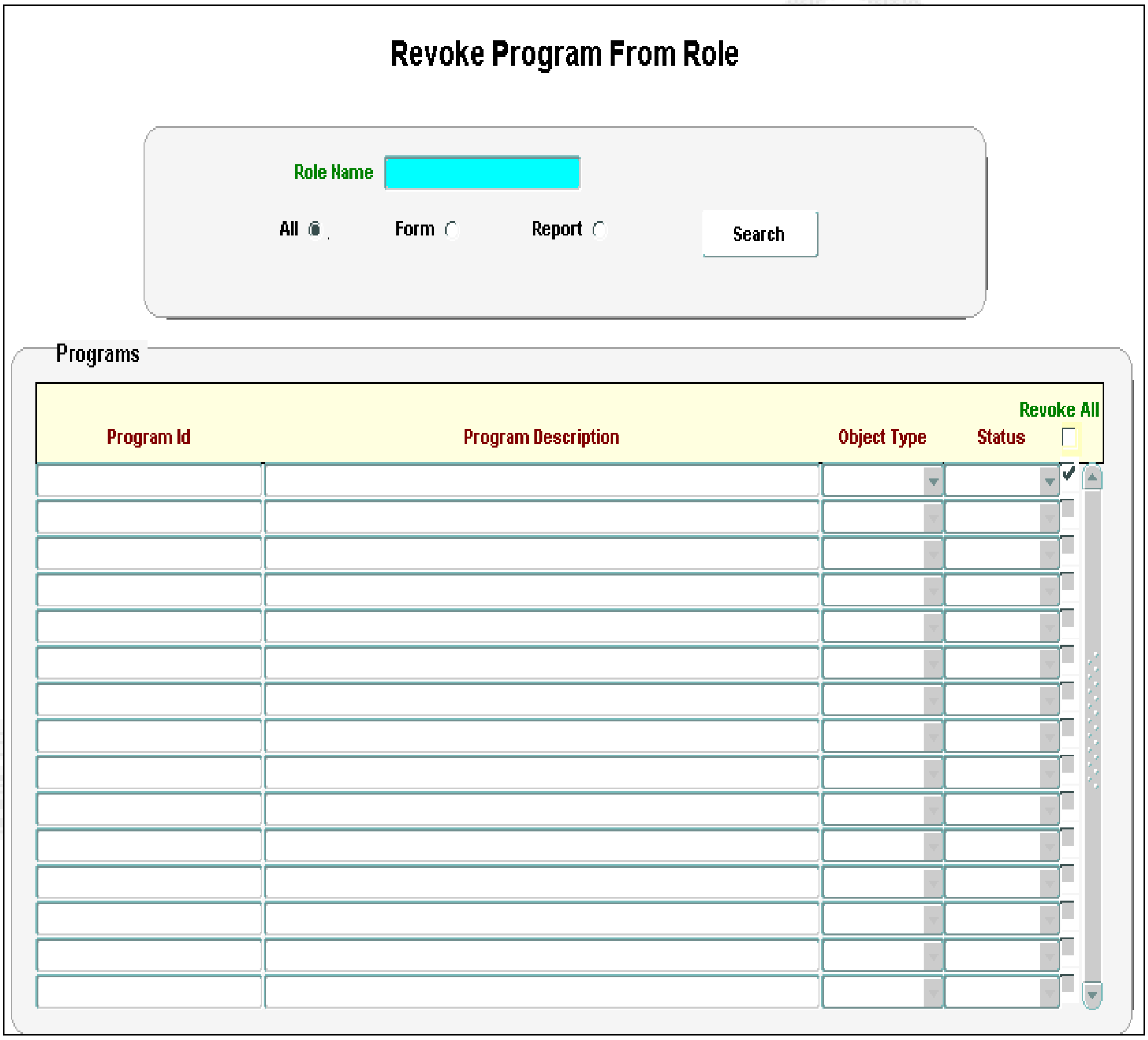
This process is initiated to revoke program from role privilege.

Big Picture:

Revoke Program From Role Privilege

11.2. Follow Steps

1 Go to the **Security** menu, select **Security Administration → Revoke Program From Role**, the screen will be displayed.



2 Enter **Role Name by** pressing F9 and select a user from the list.
3 Select **Radio** buttons either All or Form or Report respectively.
4 Click **Search** button to retrieve the data requested.
5 **Revoke all** check box will choose all the program id's**.** If user needs to revoke only few Program ID's please use individual check boxes**.**
6 Click **Save** button to save your information.
7 Click **Exit** button to exit.

11.3. Screen Glossary

Fields	Description
Role Name	Roles assigned to this user.
All/ Form/ Report radio buttons	Select the appropriate value to retrieve the requested details.
Program ID	Shows the program identification
Program Description	Shows the program type.
Object Type	Indicates either form or report.
Status	Shows status record as active or inactive.
Revoke All check box	If the checkbox is marked, this indicates that the corresponding role is revoked from this user. User has the choice to use this "Revoke All" option or to choose selected objects by ticking individual check boxes.

11.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

12. Security Administration (Revoke Privilege)

12.1. Description

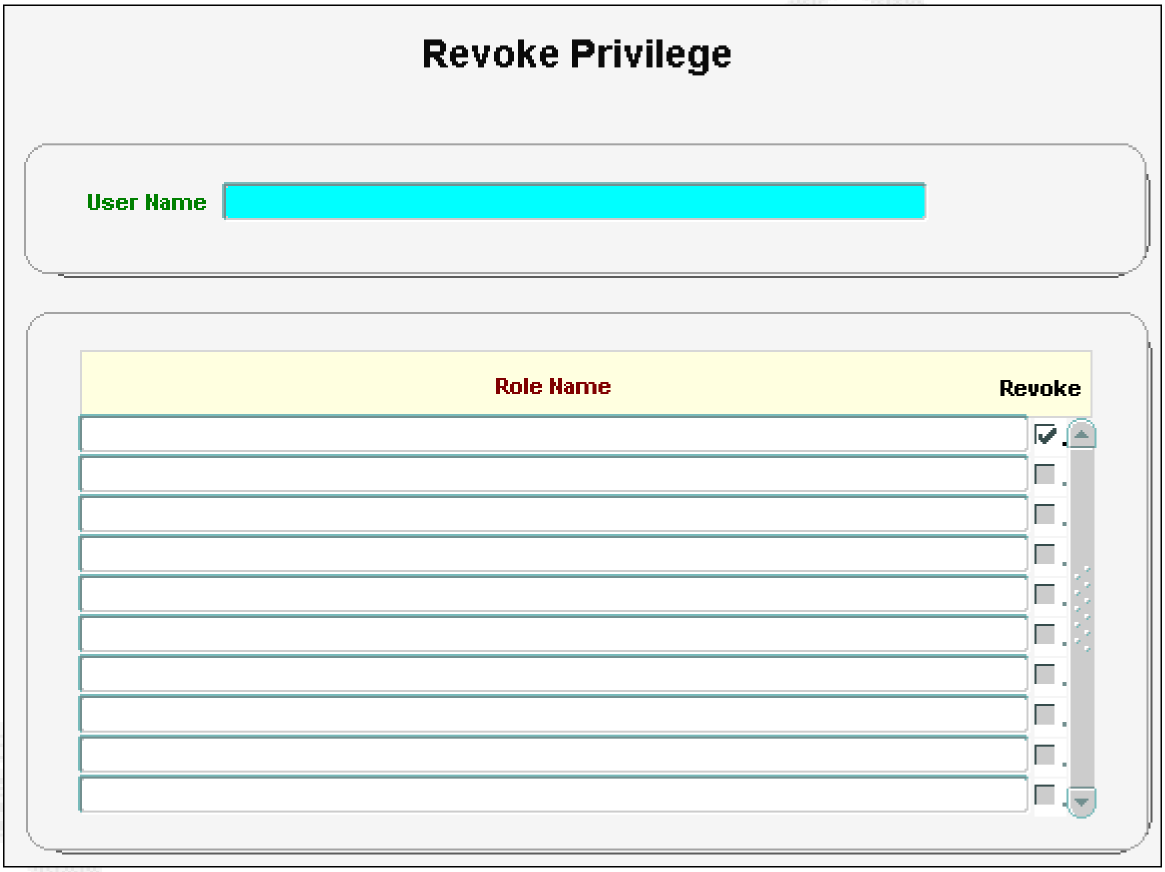
This process is initiated to revoke roles from a user.

Big Picture:

Revoke Privilege

12.2. Follow Steps

8 Go to the **Security** menu, select **Security Administration → Revoke Privilege**, the screen will be displayed.



10. Enter **User Name,** or press F7, then Press F9 and select a user from the list. Then press F8 key to retrieve details. Roles assigned to this user will be displayed. Press Up and Down arrow keys to move to the next record.
11. Mark the **Revoke** checkbox to revoke privilege from the user.
12. Click **Save** button to save your information.
13. Click **Exit** button to exit.

12.3. Screen Glossary

Fields	Description
User Name	User name.
Role Name	Roles assigned to this user.
Revoke	If the checkbox is marked, this indicates that the corresponding role is revoked from this user.

12.4. Error Messages

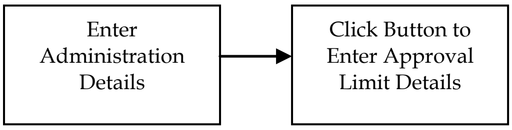
No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

13. Security Administration (User Administration)

13.1. Description

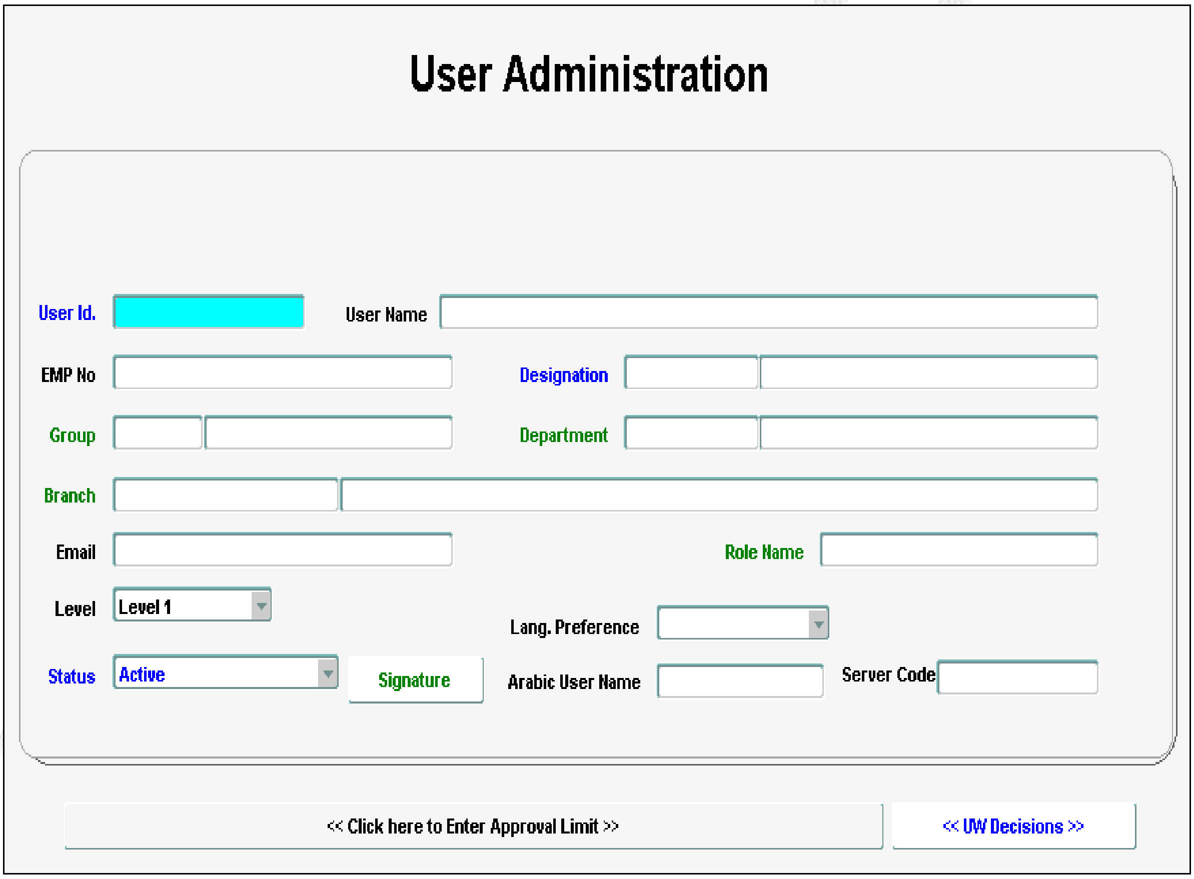
This process is initiated for user administration purposes.

Big Picture:



13.2. Follow Steps

1. Go to the **Security** menu, select **User Administration**, the screen will be displayed.

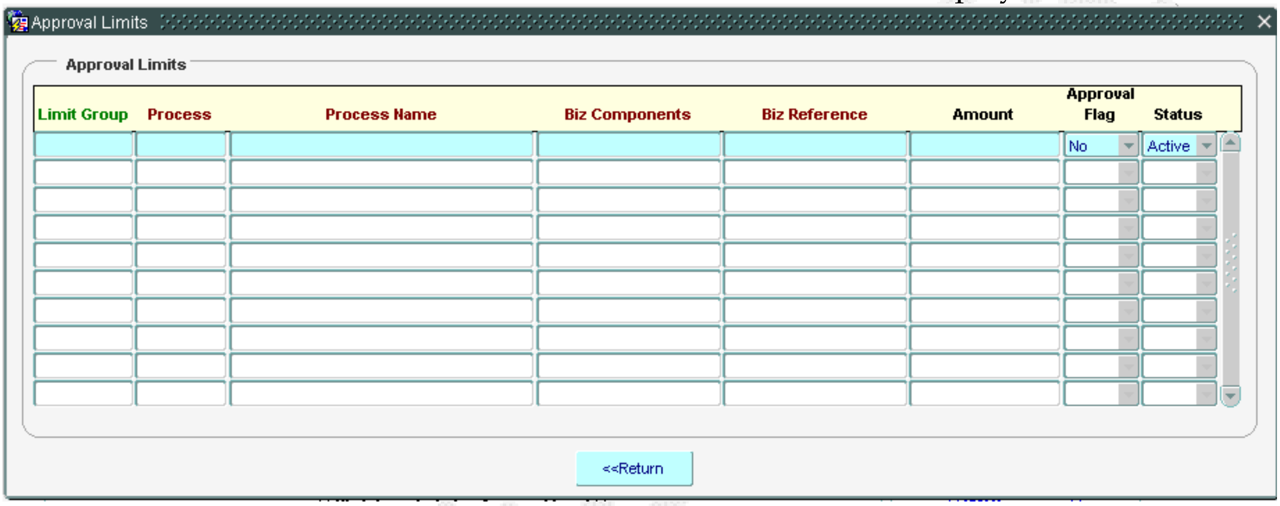


2. Enter **User ID**.

☞	**Tips** Users will be created in Oracle. All user Ids will be made available in the application.

3. Enter **EMP No**.

4. Enter **Designation** of the employee.
5. Enter **Group** which the employee belongs.
6. Enter **Department.**
7. Enter **Branch.**
8. Enter **Email** address.
9. Enter **Role Name.**
10. For non-life, select **Level** of the user.
11. Select **Lang. Preference** (language preference).
12. Enter **Status** of the record whether it is **Active** or **Inactive.**
13. Click [Signature] button to attach user signature.
14. Click [<< Click here to Enter Approval Limit >>] button, the screen will be displayed.

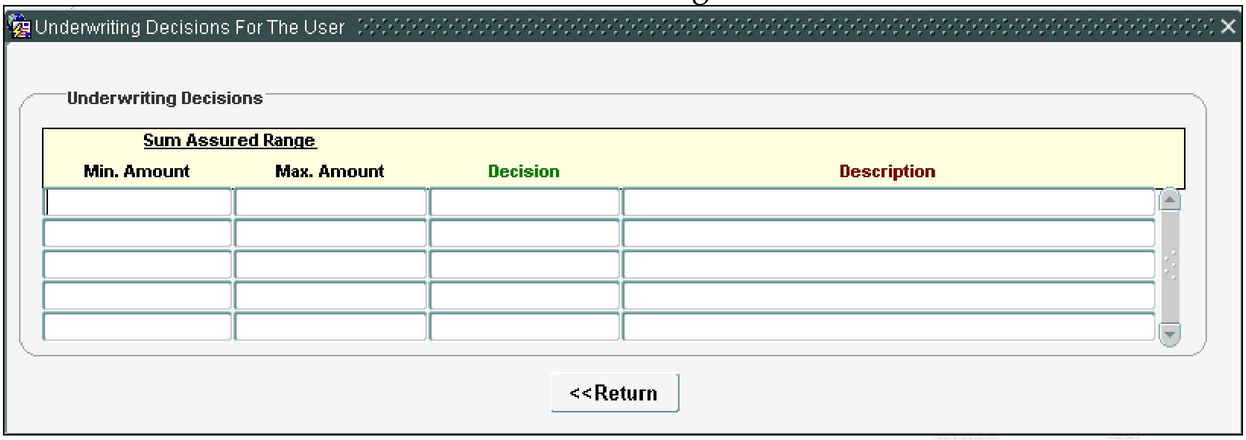


Enter **Limit Group** of this user. This defines that the user belongs to the limit group for this particular process. **Process** will be populated.

☞	**Tips** When you see [List of Values] in the status bar, you can press **F9** to see the list of values.

- Enter **Amount.**
- For Non-Life, select the **App Flag.** If yes is selected, this means that this user has the authority to approve the process.
- Select **Status,** whether it is **Active** or **Inactive.**
- Click [X] button to exit.

15. Click **UW Decisions** button to enter underwriting decisions for the user.



16. Click **Save** button to save your information.
17. Click **Exit** button to exit to the main menu screen.

13.3. Screen Glossary

Fields	Description
User ID	User ID used for application logon.
EMP No	Employee number.
Designation	User designation.
Group	Group that the user belongs.
Department	Department of the user.
Branch	Branch where the user is working.
Email	Email address of the user.
Role Name	Role assigned to the user for access control.
Level	User level.
Lang. Preference	User's language preference.
Status	Status of the record.
Signature	Signature file of the user.
Approval Limit	
Limit Group	Limit group of the user.
Process	Limit group process.
Biz Components	Business component.
Biz Reference	Business reference.
Amount	Maximum allowed amount.
App Flag	Approval flag. If yes is selected, this means that this user has the authority to approve the process.
Status	Status of the record.
UW Decisions button	
Sum Covered Range (Min. Amount/ Max. Amount)	Sum covered range.
Decision	Underwriting decision applicable for this user, for the particular sum covered range.
Description	Description of the decision.

13.4. Error Messages

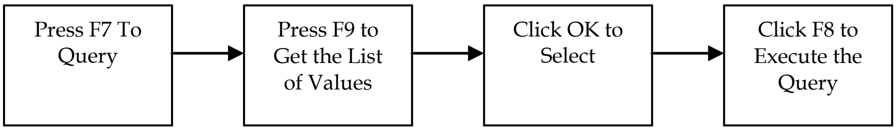
No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

14.Security Administration (User Enquiry)

14.1. Description

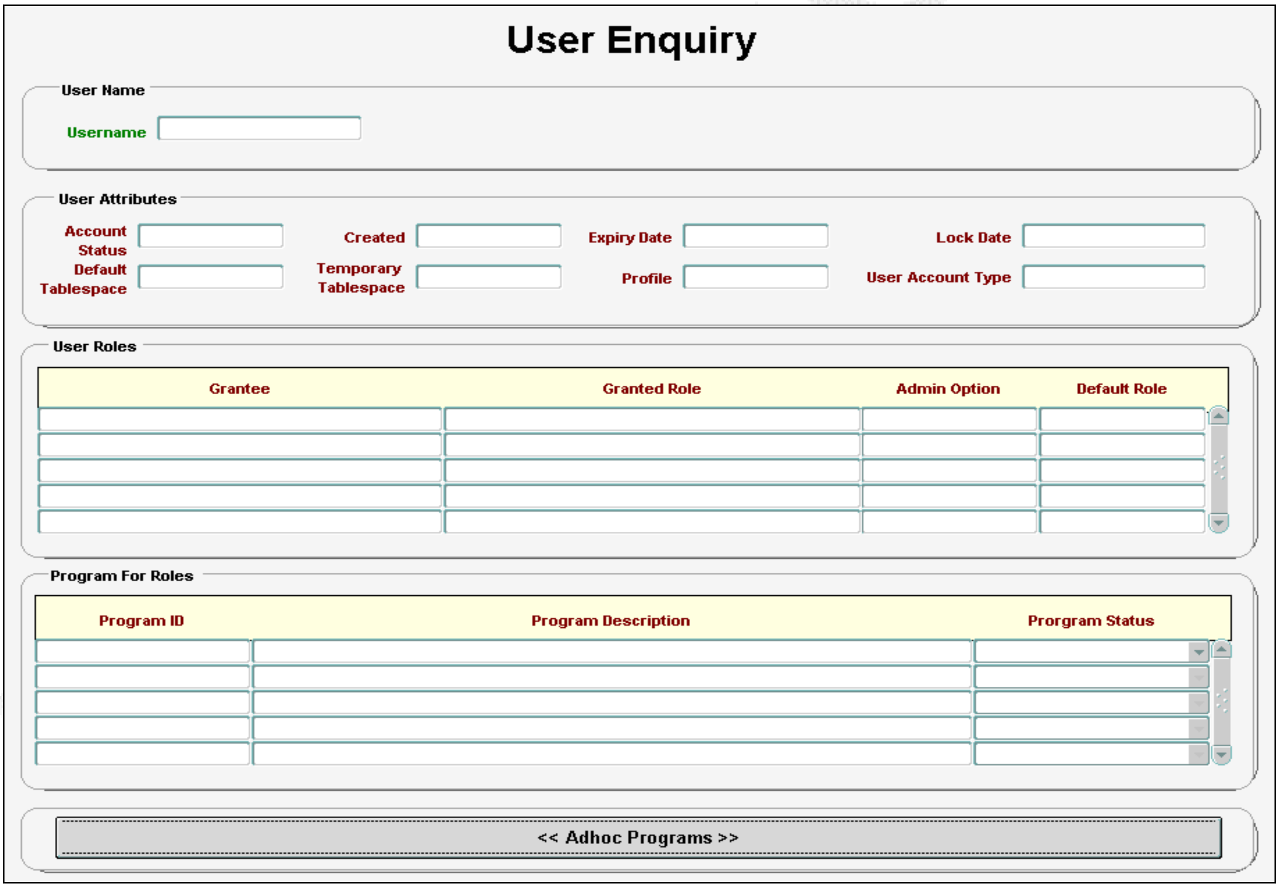
This process is initiated to perform an enquiry on user, role and privilege activities.

Big Picture:



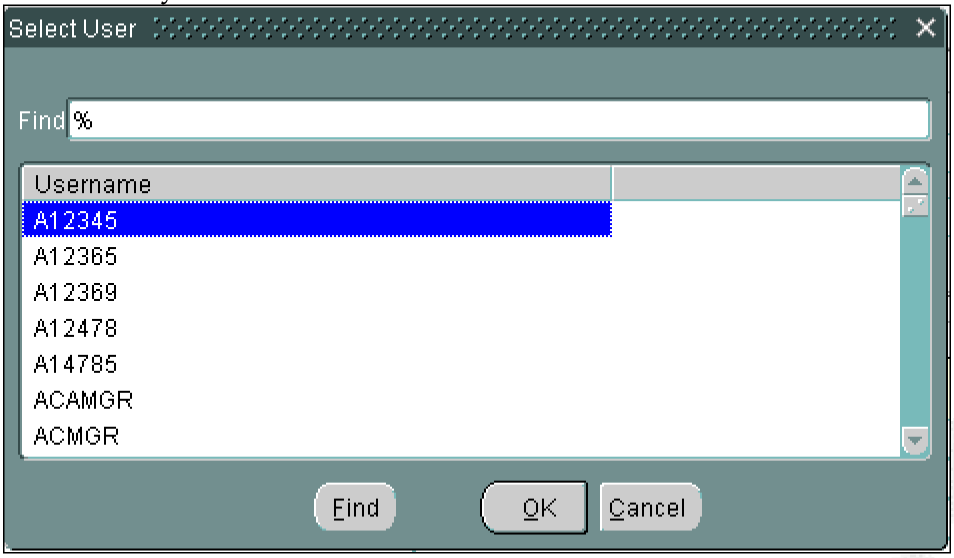
14.2. Follow Steps

1. Go to the **Security** menu, select **Security Administration → User Enquiry**, the screen will be displayed.



2. Press **F7** key to get into query mode.

3. Press **F9** key to select a user name from the list of values.

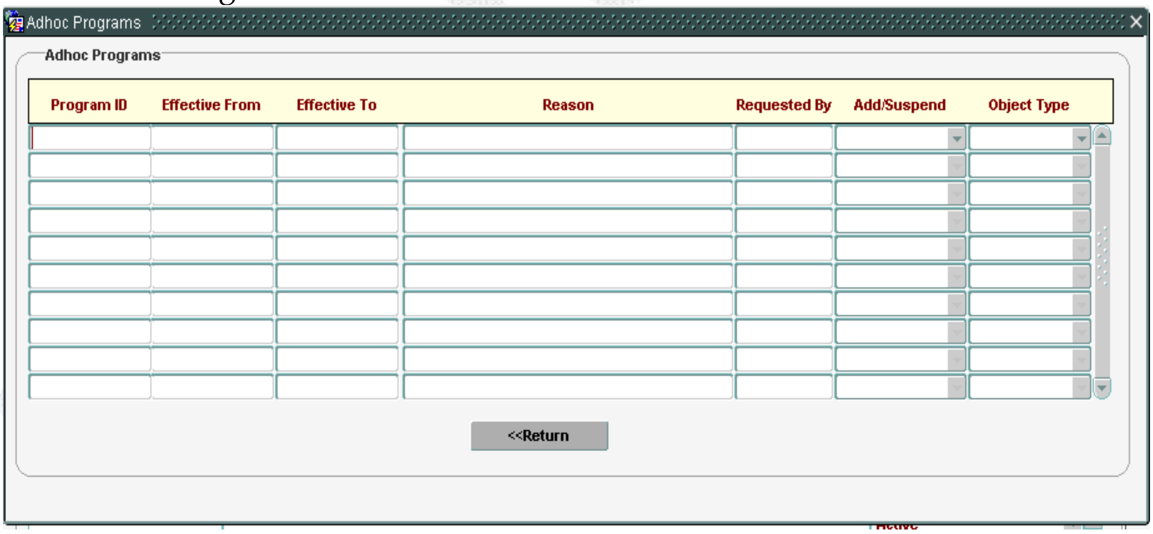


Click **OK** button to accept the selection.

4. Press **F8** key to retrieve details.
The details will be retrieved. **User Attributes** and the **User Roles** sections are populated. The **Program for Roles** details will be populated when you click on the particular role in the **User Role** section.

5. Click 

button to view the Ad-hoc Program details.



6. Click **Exit** button to exit.

14.3. Screen Glossary

Fields	Description
Username	User name.
User Attribute	
Account Status	This indicates the user status. Lock / Open / Expire/ Lock etc. **Lock**: To indicate that the user name will be locked if the user enters the password wrongly for 3 times. **Unlock**: To indicate that the user name will not be locked if the user enter the password wrongly for 3 times or more.
Created	Date on which the user name was created.
Expiry Date	Date on which this user account will expire.
Lock Date	Date on which the account was locked.
Default Tablespace	The Default Tablespace for the user. To indicate that the objects owned by the user will be created.
Temporary Tablespace	To indicates tablespace area which will be used for doing the temporary operation such as sorting a data or grouping a data.
Profile	Profile is a security feature which controls the following security options: • IDLE_TIME: how long a user can be idle after connecting to the database • CONNECT_TIME: how long a user can be connected to the database • FAILED_LOGIN_ATTEMPTS: how many failed login attempts are allowed for the user • PASSWORD_LIFE_TIME: how long a password is valid before it is forced to be changed • PASSWORD_REUSE_TIME: how many times gap a password can be reused • PASSWORD_REUSE_MAX: how many times a password can be repeated • PASSPWORD_VERIFY_FUNCTION: how complex the password should be • PASSWORD_LOCK_TIME: duration of account lock time after failed login attempts • PASSWORD_GRACE_TIME: grace time before user should change his password

User Roles	
Grantee	User.
Granted Role	Role granted to this user.
Admin Option	This indicates whether the role is granted with admin privilege or not.
Default Role	This indicates whether the role granted is a default role or not.
Program for Roles	
Program ID	Program ID applicable for this role.
Program Description	Program name applicable for this role.
Program Status	Status of the program identification.
Adhoc Programs button To show ad-hoc program assigned to users.	
Program ID	Shows the Program identification for Reports or Forms.
Effective From / Effective To	Show the effective date range from and to.
Reason	Reason for the ad-hoc program.
Requested By	The person who request the ad-hoc program
Add/Suspend	Indicates whether to add or suspend the ad-hoc program.
Object Type	Indicates Object Type is either report or form.

14.4. Error Messages

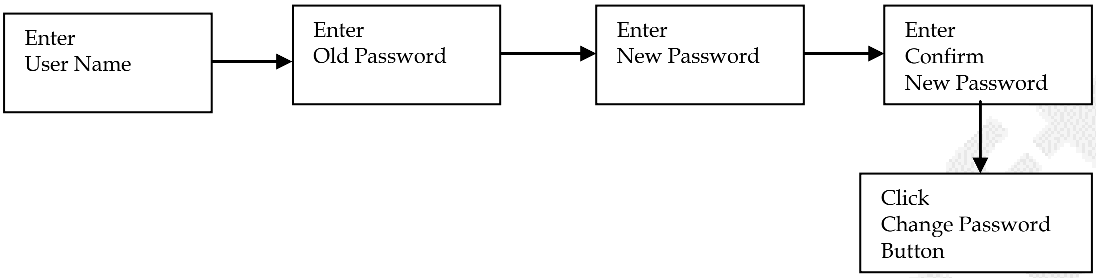
No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

15. Security Administration (Password Change)

15.1. Description

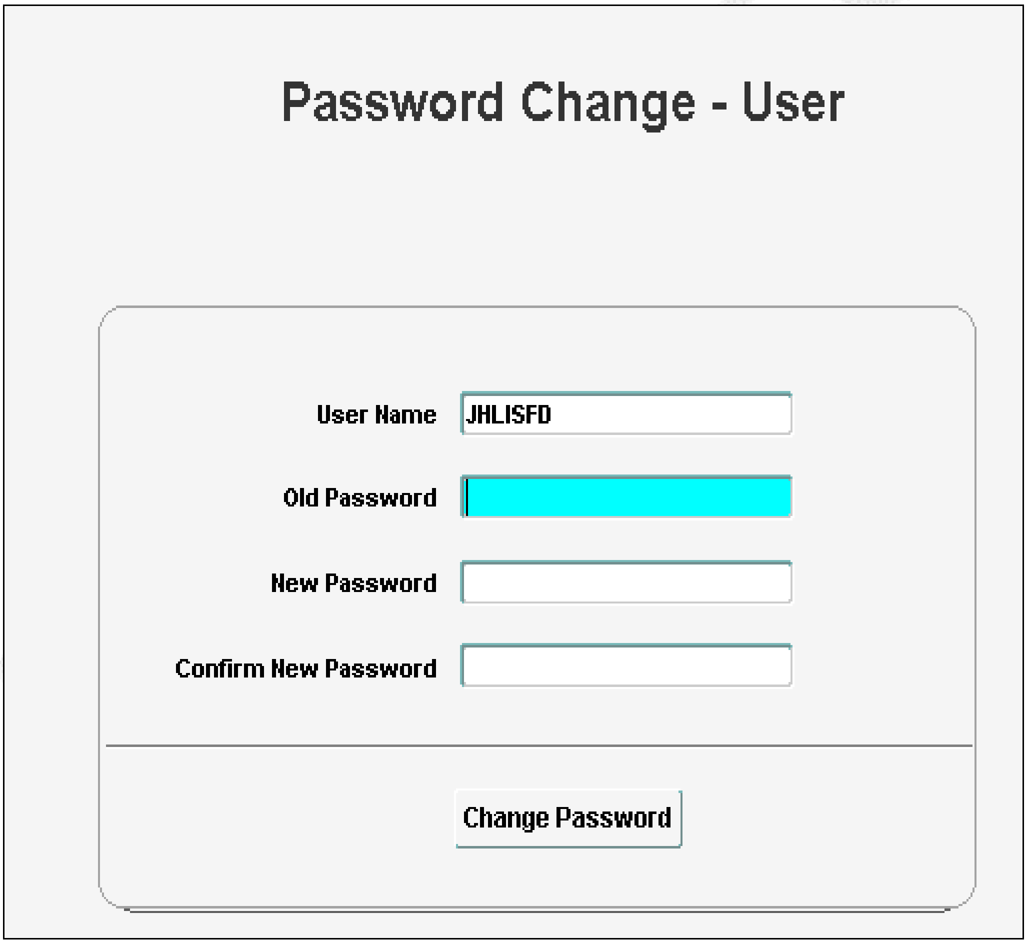
This process is initiated to change user password.

Big Picture:



15.2. Follow Steps

1. Go to **Security** menu, select **Password Change**, the screen will be displayed.



☞	**Tips** You will not be able to change the **User Name**.

2. Enter **Old Password**.
3. Enter **New Password**.
4. Enter **Confirm New Password**.
5. Click **Change Password** button to change your password.
6. Click **Exit** button to exit.

15.3. Screen Glossary

Fields	Description
User Name	User ID which you use to logon to the system.
Old Password	Your existing password.
New Password	Your new password that you want to change to.
Confirm New Password	Re-enter your new password to confirm.

15.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	Invalid User ID, or Old Password. Please re-enter.	You have entered an invalid user id or old password.	Enter a valid user name/ user ID and a valid password for the user ID.
2.	New password and confirmed password are not same. Please retype.	The New Password and Confirmed Password are not the same. Please re-enter.	Enter the same New Password and Confirmed Password.

16. Security Administration (Task Enquiry)

16.1. Description

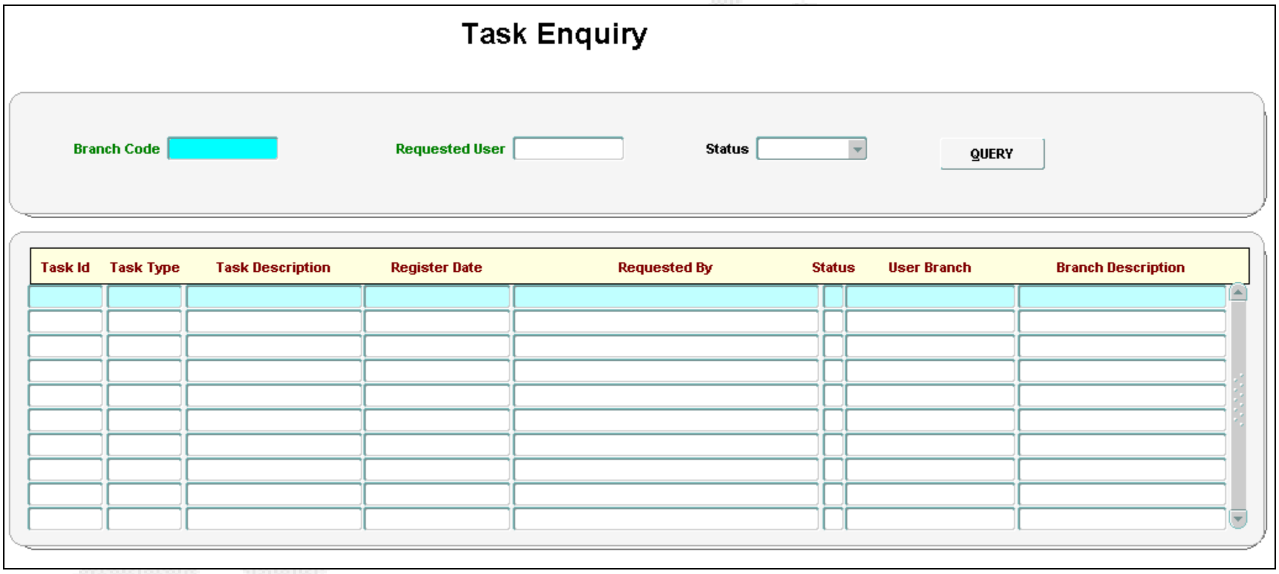
This process is initiated to perform enquiry on a task, such as Create User, Create Role, Grant Privilege, Modify Password, Clone User etc.

Big Picture:

Perform Task Enquiry

16.2. Follow Steps

1. Go to the **Security** menu, select **Security Administration → Task Enquiry**, the screen will be displayed.



2. Enter **Branch Code**.
3. Enter **Requested User**.
4. Click **Query** button to retrieve details.
5. Click **Exit** button to exit.

16.3. Screen Glossary

Fields	Description
Branch Code	Branch code.
Requested User	User who requested for the task.
Status	The status of the task, i.e. Active/ Inactive.
Task ID	A unique number which is tagged to the task.
Task Type	The type of task, for example Grant Privilege, Create User, Clone User etc.
Task Description	Task type description, such as create user, create role, grant privilege, modify password etc.
Register Date	The request date for the task.
Requested By	The person who requested for this task.
Status	The status of the task, whether active or inactive.
User Branch	Branch of the user who requested for this task.
Branch Description	Branch name.

16.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

17.Security Administration (Task Deletion)

17.1. Description

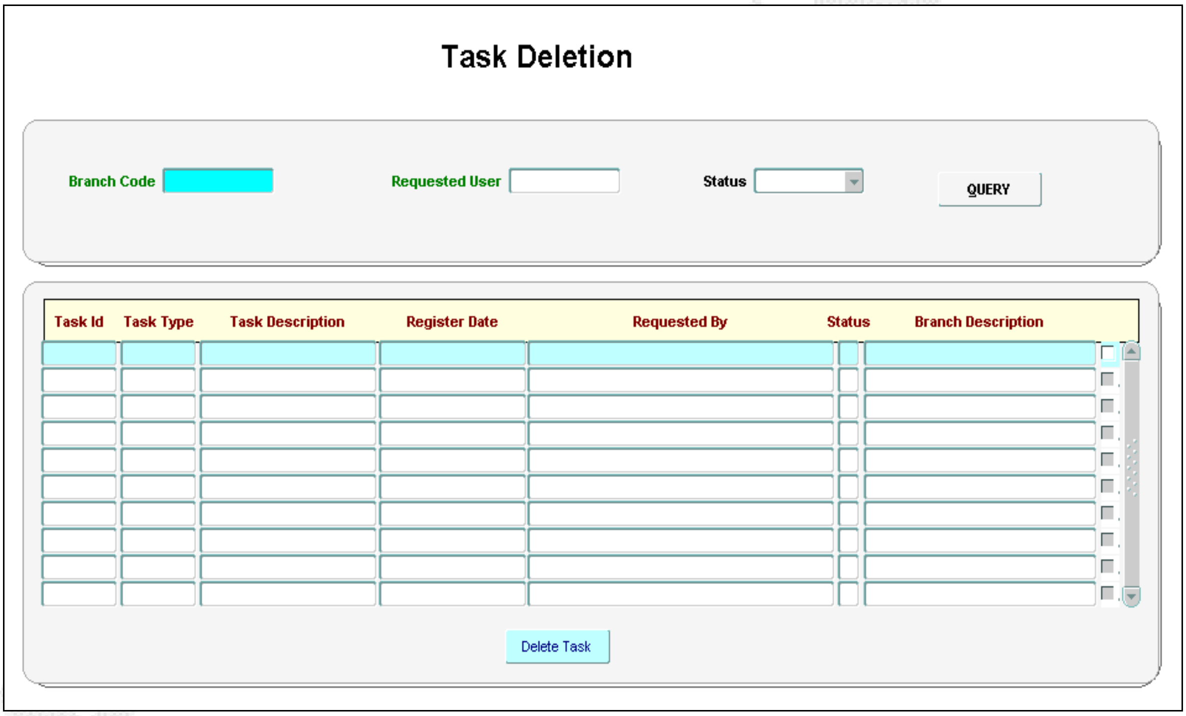
This process is initiated to delete a task.

Big Picture:

Perform Task Deletion

17.2. Follow Steps

1. Go to the **Security** menu, select **Security Administration → Task Deletion**, the screen will be displayed.



2. Enter **Branch Code**.
3. Enter **Requested User**.
4. Click **Query** button to retrieve details.
5. To delete a task, mark the corresponding checkbox, click **Delete Task** button to delete the task.
6. Click **Exit** button to exit.

17.3. Screen Glossary

Fields	Description
Branch Code	Branch code.
Requested User	User who requested for the task.
Status	The status of the task, i.e. Active/ Inactive.
Task ID	A unique number which is tagged to the task.
Task Type	The type of task, for example Grant Privilege, Create User, Clone User etc.
Task Description	Task type description, such as create user, create role, grant privilege, modify password etc.
Register Date	The request date for the task.
Requested By	The person who requested for this task.
Status	The status of the task, whether active or inactive.
User Branch	Branch of the user who requested for this task.
Branch Description	Branch name.
☑	To delete the task, mark the corresponding checkbox.

17.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A

18.Security Administration (Report Queue Manager)

18.1. Description

This master setup is used to hold all the long running reports that are in queue by the user.

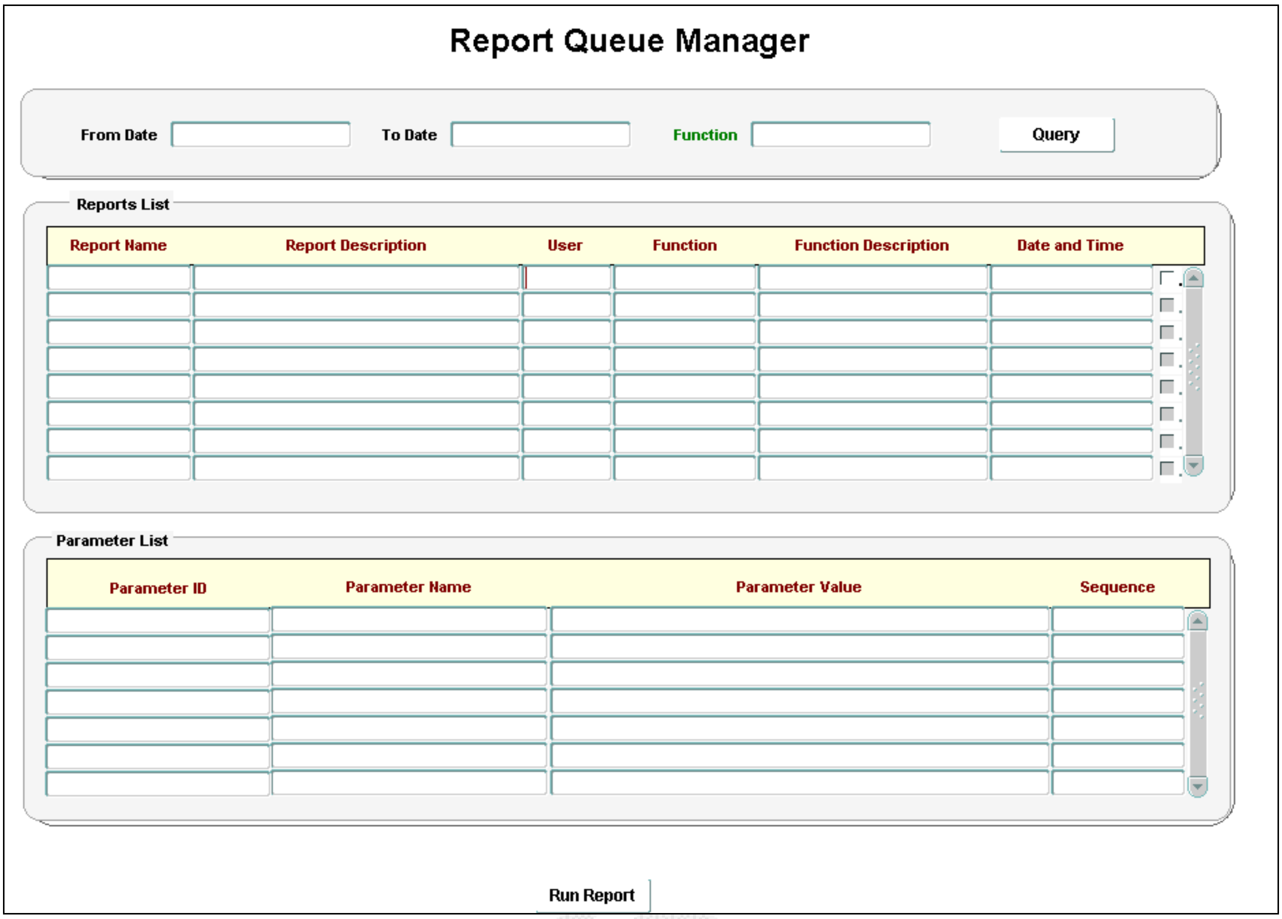
Note:
1. If any user wants to put a report to the queue other than those are listed as long time running reports they have to update V_LONG_RUN column in IS_REPORT_MASTER to 'Y' for that report ID.
2. User are must run only one report at a time as multiple running of reports are not encouraged.
3. Operator cannot change the parameter values.

Big Picture:

Perform Report Queue

18.2. Follow Steps

1. Go to the **Security** menu, select **Security Administration → Report Queue Manager**, the screen will be displayed.



2. Enter **Program Description**.
3. Enter **From Date** and **To Date**.
4. Enter **Function**.
5. Click **Query** button to display all the information.
6. Click **Run Report** button.
7. Click **EXIT** icon.

18.3. Screen Glossary

Fields	Description
Report Queue Manger	
From Date/ To Date	Show the date range selection from and to.
Function	Show the functions based on the menu, like New Business, Agency, Claims, Security, Plan Wizard, etc.
Query button	Once users press the Query button, If From Date/ To Date and function fields are empty it will display all the reports those are in the report queue manager. There are two blocks in the form. • Reports List block shows report list those are in the queue. • Parameter List block will show all the parameters relating respective reports with the values submitted by the users. By selecting one report at a time and press the **run report button** operator will be able to generate the report.
Reports List Shows all the Reports listing that are in queue.	
Report Name	Name of the report.
Report Description	Shows report description based on the report name entered earlier.
User	Shows the user who has requested for the report(s).
Function	Show the functions based on the menu, like New Business, Agency, Claims, Security, Plan Wizard, etc.
Function Description	Show the function description based on the menu.
Date and Time	Show the date and time when the user requested for the report(s).
Check Box	Place a tick in the check box to indicate which reports that requires to be generated.
Parameter List	
Parameter ID	Parameter Identification.
Parameter Name	Parameter Name.
Parameter Value	Parameter Value.
Sequence	Sequence Number.
Run Report	Use this button to run the report.

18.4. Error Messages

No.	Error Message	Reason	How to Solve
1.	N/A	N/A	N/A