Security User Guide

Oracle FLEXCUBE Investor Services

Release 12.0.3.4.0

May 2018

ORACLE

Table of Contents

1. About This Manual

1.1 Introduction

Welcome to Oracle FLEXCUBE Investor Servicing ™, a comprehensive mutual funds automation software from Oracle Financial Servicing Software Ltd. ©.

This Oracle FLEXCUBE Investor Servicing User Manual helps you use the system to achieve optimum automation of all your mutual fund investor servicing processes. It contains guidelines for specific tasks, descriptions of various features and processes in the system and general information.

1.2 Related Documents

The User Manual is organized in to various parts, each discussing a component of the Oracle FLEXCUBE Investor Servicing system.

1.3 Audience

This Fund Manager User Manual is intended for the Fund Administrator users and system operators in the AMC.

1.4 Organization

This volume of the Fund Manager User manual is organized under the following chapter sequence:

Chapter 1	*About This Manual* explains the structure, audience, organization, and related documents of this manual.
Chapter 2	*Security – Ensuring Security* explains how to use the system as an authorized user and also manage the other users that can access the system.
Chapter 3	*Security – Enabling Auto Authorization* explains why authorization is required and how to enable auto authorization and its features.

1.5 Conventions Used in this Manual

Before you begin using this User Manual, it is important to understand the typographical conventions used in it.

1.5.1 General Conventions

Convention	Type of Information
Italic type	Functional /foreign terms Validations for fields on a screen References to related Headings/Users Manuals For emphasis
Numbered Bullet	Step by step procedures

1.5.2 Keyboard Conventions

Convention	Type of Information
Keys	All keys of the keyboard are represented in capital letters. For example, <CTRL>.
Shortcut keys	All short cut keys are contained in brackets. For example, <ALT+SHIFT>.

1.6 Glossary of Icons

This User Manual may refer to all or some of the following icons.

Icons	Function
	Exit
	Add Row
	Delete Row
	Option List

Refer the Procedures User Manual for further details about the icons.

1.7 Abbreviations and Acronyms

The following acronyms and abbreviations are adhered to in this User Manual:

Abbreviation/ Acronym	Meaning
ADMIN	User Administrator
AGY	The Agency Branch component of the system
AMC	Asset Management Company
BOD	Beginning of Day
CDSC	Contingent Deferred Sales Charge

Abbreviation/ Acronym	Meaning
CGT	Capital Gains Tax
CIF	Customer Information File
EOD	End of Day
EPU	Earnings per unit
FC-IS	Oracle FLEXCUBE Investor Servicing
FMG	The Fund Manager component of the system
FPADMIN	Oracle FLEXCUBE Administrator
ID	Identification
IHPP	Inflation Hedged Pension Plan
IPO	Initial Public Offering
LEP	Life and Endowment Products
LOI	Letter of Intent
NAV	Net Asset Value
REG	The Registrar component of the system
ROA	Rights of Accumulation
ROI	Return on Investment
SI	Standing Instructions
SMS	Security Management System
URL	Uniform Resource Locator
VAT	Value Added Tax
WAUC	Weighted Average Unit Cost

1.8 Getting Help

Online help is available for all tasks. You can get help for any function by clicking the help icon provided or by pressing F1.

2. Ensuring Security for Fund Manager

2.1 Introduction

In any financial environment, security of information is of paramount importance. Access to information must be made available in a carefully monitored manner. Controlling and maintaining these aspects also includes management of the people (or users) who will process this information on a day to day basis. Therefore, an efficient Security Management System is an important factor that will determine the strength and stability of a financial system.

This chapter takes you through the Security Maintenance features of the Oracle FLEXCUBE system. You will learn how to use the security features in the system to suit your requirements and customize them for your environment.

This chapter is intended for the following persons in your bank or AMC:

Person	Operation
Oracle FLEXCUBE Implementers	To set up the initial start-up parameters in the individual client workstations. To set up security management parameters for the AMC or AMC branch.
SMS Administrator for the Bank/ AMC	To set the SMS AMC or AMC branch parameters. To identify the Branch level SMS Administrators.
SMS Administrator for the Branch	To create User and Role profiles for the branches of your AMC. Will also grant access to the various functions to the Users.
A Oracle FLEXCUBE user	Any user of Oracle FLEXCUBE whose activities are traced by the Security Management System.

2.2 Security Management

In Oracle FLEXCUBE, you can ensure security management at all levels in any kind of environment. This is due to a combination of the following features:

- User-level Access Control
- Business function-level Access Control
- Operation-level Access Control

Simply translated, this means that a person within your environment can:

- Only access the system as an authorized user
- Only access certain allowed functions within the system
- Only perform certain allowed operations on the function for which access is allowed

2.3 Some Important Terms

Before you operate the security management system of your Oracle FLEXCUBE installation, you must understand some important terms that you will encounter during the process.

2.3.1 System Administrators

Typically, at the time of installation, two users are created by default in the system database. These two users are the system administrators. The system administrators subsequently create all users and user roles in the system,

The system administrator user profiles would be typically created to enable the security managers in your bank or AMC, to log in to the system.

2.3.2 Functions

A function is any operation related to business maintenance or processing in the system. Most typically, each menu item appearing in the main menu could be thought of as a function. For a user, you can control access to different functions in the system.

Any functions related to the Fund Manager component can be thought of as back office functions, and any functions related to the Agency Branch could be thought of as front office components.

The functions are made available by the Oracle FLEXCUBE implementers, at the time of installation.

2.3.3 User Profile

Each user who will use the system is given a unique profile in the database. This profile is known as a user profile.

The profile of a user contains the User ID, the password and the functions to which the user has access. A user can be assigned access to either back office (Fund Manager) functions, or front office (Agency Branch) functions, depending upon the tasks that the user must perform in your organization.

2.3.4 Roles

It is likely that users working in the same department at the same level of hierarchy need to have similar user profiles. In such cases, you can define a Role Profile, which includes access rights to the functions that are common to a group of users. A user can be linked to a Role Profile by which you give the user access rights to all the functions in the Role Profile.

A role profile could contain either back office (Fund Manager) functions or front office (Agency Branch) functions.

2.4 Other Features of Security Management System

2.4.1 Restricted Number of Unsuccessful Attempts

You can define the maximum number of unsuccessful attempts after which a User ID should be disabled. The password of a user can be made applicable only for a fixed period. This forces the user to change the password at regular intervals thus reducing security risks. Further, you can define passwords that could be commonly used by a user as Restrictive Passwords at the user, user role and bank level. A user cannot use any password that is listed as a Restrictive Password at any of these levels.

2.4.2 Restricted Access to Branches

You can indicate the branches from where a user can operate. Click on the User Branch Restrictions button in the User Profile Definition screen to define the branches from where a user can operate.

2.4.3 Restricted Access to AMC Branches

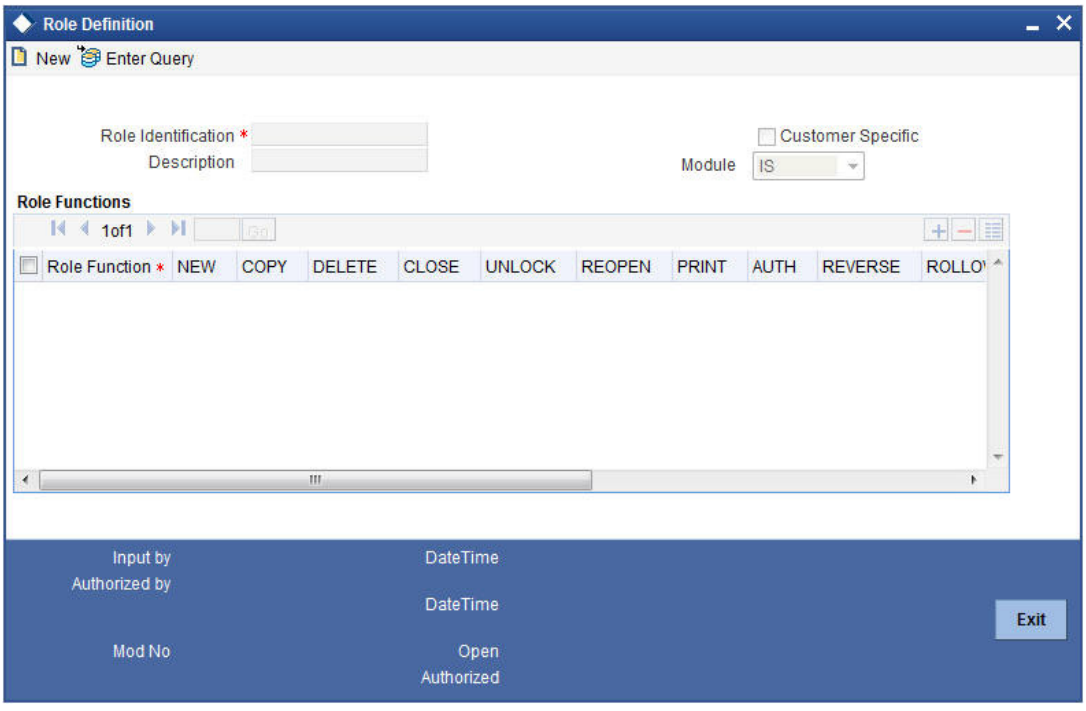
For mutual fund account customers, you can indicate the branches of the AMC from where a user can operate. Click on the Module button in the User Profile Definition screen to define the branches of the AMC from where a user can be allowed to operate.

2.4.4 All Activities Tracked

Extensive log is kept of all the activities on the system. You can generate reports on the usage of the system anytime. These reports give details of unsuccessful attempts at accessing the system along with the nature of these attempts. It could be an unauthorized user attempting to use the system, an authorized user trying to run a function without proper access rights, and so forth.

2.5 Defining Role Profiles

Role profiles are defined in the Role Definition screen. You can invoke the 'Role Definition' screen by typing 'SMDROLDF' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button. The screen is displayed below:



2.5.1 Fields in Role Definition Screen

Role Identification

Alphanumeric, Mandatory

Specify a unique identifier for the role profile.

Description

Alphanumeric, Mandatory

This is the key text which describes and qualifies the role profile, and is indicative of its characteristics.

Customer Specific

Optional

Check this box to indicate that the role profile has been set up for a specific customer of your AMC or AMC branch who might access the system from a remote terminal to inquire about their transactions or investor accounts.

Module

Optional

Select the default module for users linked to the role profile.

Role Functions

After you have defined the basic attributes of a role profile (the Role ID, Description, Module and whether it is customer- specific) you should define the functions to which the role profile has access. The various functions in the system fall under five categories, corresponding to the menu options in the Agency Branch main menu.

A role profile could contain either back office (Fund Manager) functions or front office (Agency Branch) functions.

Select the function that you want to link to the role profile.

For each function, you can allow or disallow specific record-level operations. These operations are displayed as a horizontal list, alongside the Maintenance Functions label, with each operation spelled out vertically.

In the selected function row, check the box pertaining to each operation you want to allow for the role profile.

You can allow any of the following operations at record level for the role profile in any function:

2.5.1.1 Static Tables

- New (Define a new record).
- Copy (Copy details of an existing record).
- Delete (Delete an existing record).
- Close (Close an existing record).
- Unlock (to amend an existing record).
- Reopen (Reopen an existing record).
- Print (Print the details of selected records).
- Authorize (Authorize any maintenance activity on a record).

2.5.1.2 Contracts and On-line Transaction Processing

- View (to see the details of the contract).

2.5.1.3 Reports

- Generate (to generate reports).
- View (view the reports).

- Print (print the reports).

To delete the access rights you have specified for a function, select the required Function ID row and check the Delete box at the extreme right end of the row.

To edit the access rights you have specified for a function, select the required Function ID row and check the Edit box at the extreme right end of the row.

2.5.2 Classifying Role Profile

By default, a Role Profile you define will be for the users who are employees of your AMC or AMC branch. You can indicate that the profile is for customers who might login from remote terminals to inquire on their transactions and balances.

2.5.3 Copying Role Profile of Existing Role

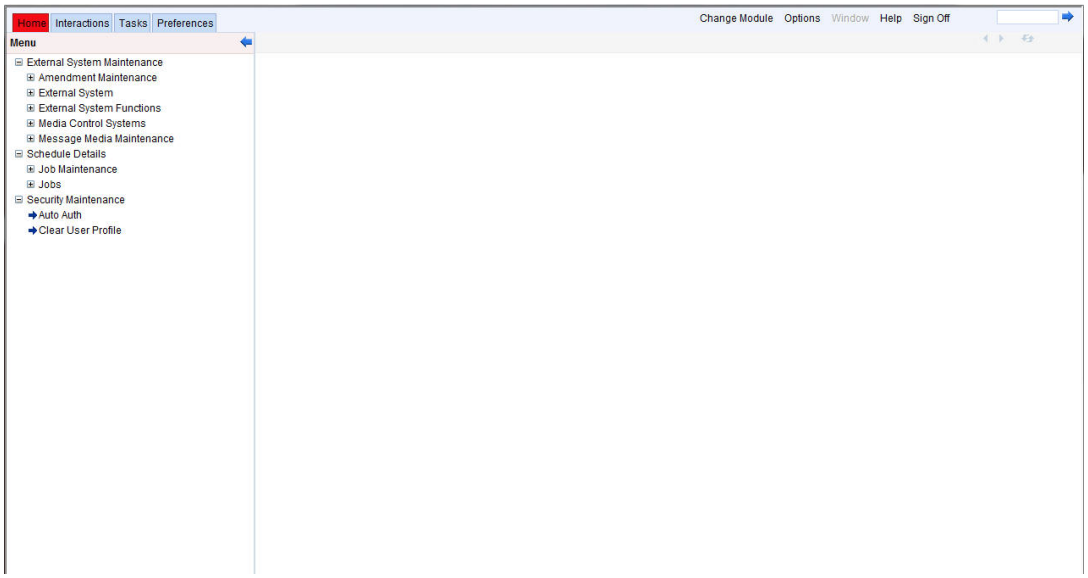
Often, you may have to create a Role Profile that closely resembles an existing one. In such a case, you can copy the existing profile on to the new one.

To copy a role, you need to retrieve the record whose attributes you wish to copy. This is done as follows:

- Click the F7 button.
- Input the Role ID.
- Click on F8.

All the details related to the particular Role Id are displayed by the system. Choose the Copy button from the row of buttons at the topmost row of the screen All the details of the profile except the Role ID will be copied and displayed. Enter a unique Role ID. You can change any of the details of the profile before saving it.

If you have retrieved an existing role profile and you want to copy it to a new role profile, click the Copy button in the topmost row of buttons in the screen. The Copy Information screen is opened, and you can specify the Role ID and Description for the new role profile.



All the details of the existing profile are copied onto the new role profile. Again, you can change any of the details of the profile before saving it.

2.5.4 Deleting Role Profile

A Role Profile should be deleted only if there are no users linked to it. Thus, before deleting a role profile, you should modify each user profile attached to it and delete the link to the role.

To delete an existing role profile, you have to retrieve the record that you wish to delete. This is done as follows:

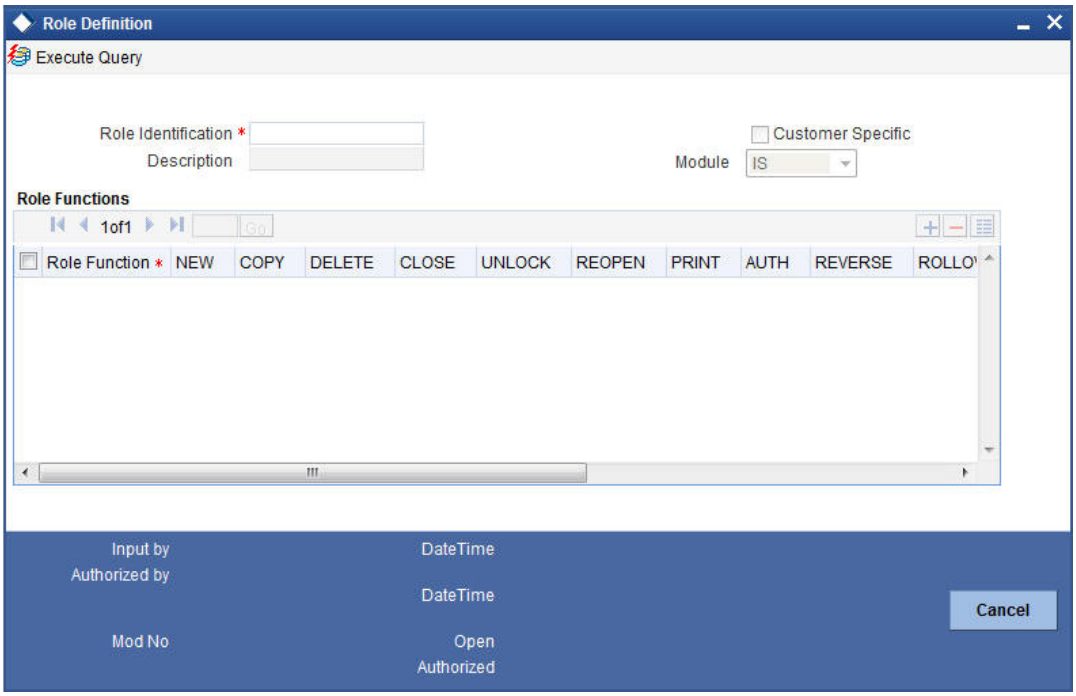
- Click the F7 button.
- Input the Role ID.
- Click on F8.

All the details related to the particular Role Id are displayed by the system. Then select the Delete button from the topmost row of buttons in the screen. If the role is linked to any user, a warning message will be displayed. This message will bring your attention to the fact that the user profile to which the role is linked will not be the same if the role profile is deleted.

You will be prompted to confirm the deletion. The Role Profile will be deleted only if you confirm the deletion.

2.5.5 Retrieving Role Profile in Role Definition Screen

To retrieve a role profile that you have previously set up in the Role Definition screen, choose the 'Query' button from the topmost row of buttons in the screen. The Query screen is opened.



- Click F7.
- Input the Role Id.
- Click F8.

All the details related to the particular Role Id are displayed by the system.

2.5.6 Authorizing Role Profile

Before you link any users to a role, a user other than the one that defined it must authorize it. To authorize a role profile,

- Retrieve the role profile record so that it is displayed in the Role Definition screen.
- Click F7, input the Role ID and click F8. All the details pertaining to the Role ID specified are displayed. Choose the Auth button from the topmost row of buttons in the screen. The Maintenance Authorization Details screen is displayed. The detail of each modification that was made to the record, in the sequence of occurrence is shown in this screen. For each modification, the following details are displayed:
  - The sequence number for the modification, in the Mod No. field.
  - The operation that resulted in the modification, the Action field.
  - The user that effected the modification, in the Input By field.
  - The time at which the modification occurred, in the Date Time field.
  - In the lower grid portion, the changed values for each modification are displayed.
  - You can authorize any of the modified records, or all of them. Check the box in the Authorize field in the desired row, to mark it for authorization.

When you have marked the required modifications for authorization, click the OK button to effect the authorization. The Maintenance Authorization Details screen is closed, and you are returned to the Role Definition screen.

2.5.7 Editing Role Profile

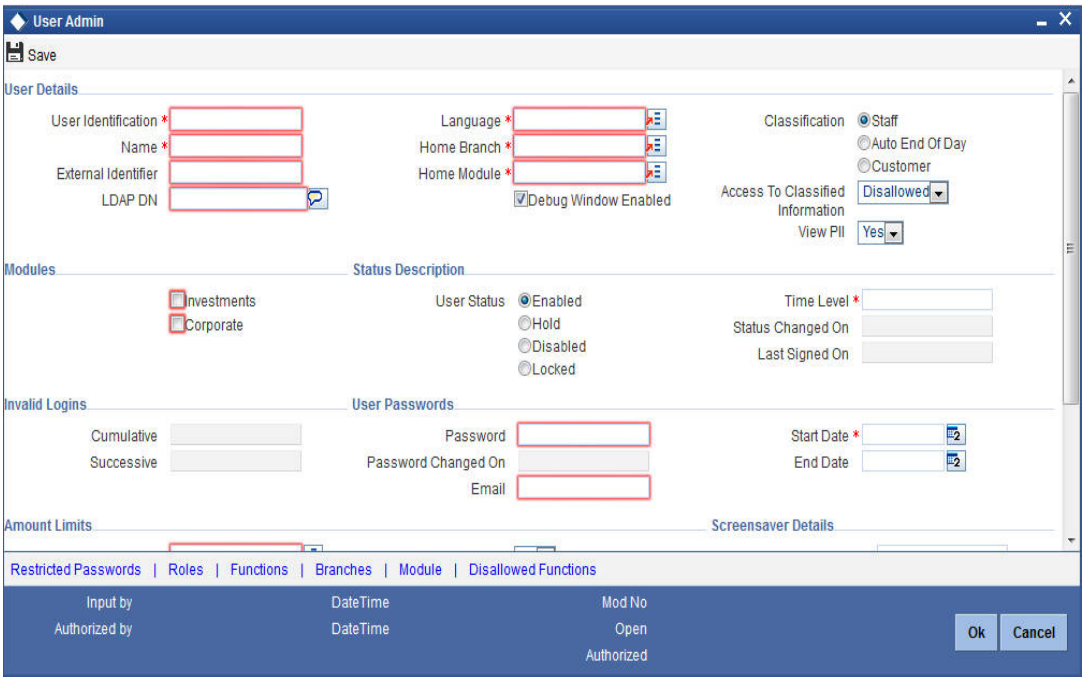
You can make changes to an authorized role profile as follows:

- Retrieve the role profile record so that it is displayed in the Role Definition screen.
- Click the Edit button from the topmost row of buttons in the screen. The record is now in readiness for modification.
- After making your changes, click the Save button from the topmost row of buttons in the screen to save your changes. The record is now an edited, unauthorized record. Another user must now authorize it for it to be effective again.

2.6 Defining User Profile

A User Profile defines the activities that a user can carry out on the system. It also contains the user ID, the name through which the user will access the system and the password.

You can invoke the ‘User Admin’ screen by typing ‘SMDUSRDF’ in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button. The screen is displayed below:



Specify the following basic information for the user profile, in the User Details section in this screen:

User Details

User Identification

Alphanumeric; 12 Characters; Mandatory

Specify a unique identifier for the user.

Name

Alphanumeric; 35 Characters; Mandatory

Specify the name of the user.

External Identifier

Alphanumeric; 20 Characters; Optional

Specify the External Identifier. External user is an alternative name for user id where two users cannot have same External identifier.

LDAP DN

Alphanumeric; 500 Characters; Optional

Specify LDAP DN details that is maintained in SSO screen.

The application will verify if only one user ID in FLEXCUBE Investor Service is mapped to the subject (DN) while authentication via SSO.

Language

Alphanumeric; 3 Characters; Mandatory

Specify the preferred language for the user profile. Alternatively, you can also select language from the option list. The list displays all valid language code maintained in the system.

Home Branch

Alphanumeric; 3 Characters; Mandatory

Specify the home branch details.

Home Module

Alphanumeric; 30 Characters; Mandatory

Specify the default module from which the user profile will operate.

Debug Window Enabled

Optional

Check this box to enable debug window.

Show Dashboard

Optional

Check this box to show dashboard.

Classification

Optional

Select one of the classification options:

- Staff
- Auto End Of Day
- Customer

You can classify a user as belonging to one of the following categories:

Staff	A user of the system who is an employee of your bank or AMC. You can include any of the functions available in the system in the user profile. Ideally, you should not include functions that are part of End of Cycle or End of Day operations in the profile of a Staff user.
Customer	A customer who would want to log into the system from a remote terminal. You can include only those functions through which the customer can inquire into balances and transactions.
AEOD	A user at the bank or AMC who is responsible for running the automated End of Day operations. You can include any of the functions available in the system in the user profile. Ideally, you should include only functions that are part of End of Cycle operations in the profile of a AEOD user.

You can indicate this through the Classification field in the User Profile Definition screen.

Access To Classified Information

Optional

Select if access to classified information is allowed or not from the drop-down list. The list displays the following values:

- Allowed
- Disallowed

View PII

Optional

Select if Personal Identifiable Information has to be viewed or not from the drop-down list. The list displays the following values:

- Yes

- No

By default, ‘View PII’ field is set to ‘Yes’.

If you select ‘No’, then you need to amend user roles with View only Roles to all ‘Personal Identifiable Information’ related screens. This is usually applicable to a user with only back-office role.

Modules

Investments

Optional

Check this box if the user is investment module user.

Corporate

Optional

Check this box if the user is corporate module user.

Status Description

User Status

Optional

Check one of the user status by checking the appropriate radio button:

- Enabled
- Hold
- Disabled
- Locked

Time Level

Numeric; 1 Character; Mandatory

Specify the time level.

Status Changed On

Display

The system displays the most recent date of status change of user profile.

Last Signed On

Display

The system displays the last logged in details

Invalid Logins

Cumulative

Display

The system displays the number of successive invalid login attempts (in a single session) after which the user ID will be disabled for this profile.

Cumulative

Display

The system displays the number of successive invalid login attempts (spread across different sessions) after which the user ID will be disabled for this profile.

After you have entered these basic details, you can specify any of the following information for the user profile, depending upon the necessity.

Note

When authentication of credentials is unsuccessful due to an incorrect user ID, then the user ID will not be logged in the audit logs. In case the user ID is correct and the password is wrong, the attempt is logged in the audit log and the successive and cumulative failure count is incremented. When the user ID and password are correct, this is logged into the audit logs.

User Passwords

Password

Alphanumeric; 32 Characters; Optional

Specify the user password to login. The static data AUTO_GEN_PASS_REQ is provided. The defaulted value 'Y' indicates whether the auto generation of the password is required or not.

Note

If the application level parameter which indicates the auto generation of the password is required or not is set to Y (Yes), then this field will be disabled and the system will create a random password in accordance with the parameters maintained at the level of the bank. The new password will be send to the respective user via mail.

At the time of setting up the Oracle FLEXCUBE Investor Servicing, the number of repeated successive parameters allowed in a password will be indicated.

For instance, if the number of repeated successive parameters allowed in a password has been set as '2', then the user password can have a character repeating only twice. Suppose, if the number of repeated successive parameters has been specified as 2, a user password like AAA777 will be invalid. A valid password would be AA77.

Password Changed On

Display

The system displays the date when the password was last changed.

Email

Alphanumeric; 50 Characters; Optional

Specify the e-mail ID of the user.

Start Date

Date Format; Mandatory

Select the start date for the user password from the adjoining calendar.

End Date

Date Format; Optional

Select the end date for the user password from the adjoining calendar.

Note

The System is also configured to disallow the use of a pre-set number of previous passwords. This pre-set number is assigned at the time of installation, as a system parameter; the number can be subsequently changed if required, by changing this system parameter.

Access Control

Optional

Select the access control from the drop-down list. The list displays the following values:

- UI
- Gateway
- Both

The system is configured to disallow the use of a pre-set number of previous passwords. This pre-set number is assigned at the time of installation. As a system parameter; the number can be subsequently changed if required by changing this system parameter.

Amount Limits

Limit Currency

Alphanumeric; 3 Characters; Mandatory

Specify the currency to be mapped for transaction amount and auth amount.

Transaction Amount

Numeric; 18 Characters; Mandatory

Specify the maximum amount value that the user can specify while entering a transaction request from an investor.

Auth Amount

Numeric; 18 Characters; Mandatory

Specify the maximum amount value of an investor transaction that the user can authorize.

Date Format

Optional

Select the date format from the drop-down list. The list displays the following values:

- M/D/YYYY
- M/D/YY
- MM/DD/YY
- YY/MM/DD
- YYYY-MM-DD
- DD-MMM-YY
- DD-MMM-YYYY
- DD/MM/YYYY
- DD-MM-YYYY

Auto Auth

Optional

Select auto authorization status from the drop-down list. The list displays the following values:

- Yes
- No

Amount Format

Optional

Select the amount format from the drop-down list. The list displays the following values:

- Dot Comma

- Comma Dot
- Comma

Number Format

Optional

Select one of the number format options to be used:

- XXX,XXX,XXX,XXX
- XX,XX,XX,XX,XXX

2.6.1 Classifying User

You can classify a user as belonging to one of the following categories:

Staff	A user of the system who is an employee of your bank or AMC. You can include any of the functions available in the system in the user profile. Ideally, you should not include functions that are part of End of Cycle or End of Day operations in the profile of a Staff user.
Customer	A customer who would want to log into the system from a remote terminal. You can include only those functions through which the customer can inquire into balances and transactions.
AEOD	A user at the bank or AMC who is responsible for running the automated End of Day operations. You can include any of the functions available in the system in the user profile. Ideally, you should include only functions that are part of End of Cycle operations in the profile of a AEOD user.

You can indicate this through the Classification field in the User Profile Definition screen.

2.6.2 Allowing User to Operate from Different Branches

When you create a User Profile, it will be attached to the branch where it is created. This means that the user can execute the functions defined for the profile from this branch. For a user profile, you can indicate that the user can access other branches also. The kind of functions a user can perform in a branch other than the one where the user profile is created depends on the category of the user.

2.6.2.1 Allowing User to Operate from Different Branches of AMC

For mutual fund account customers, you can define a list of branches of the AMC from which the user would be allowed to operate. To define this list, click the AMC button in the User Profile Definition screen.

2.6.2.2 User Belonging to Staff Category

In each branch, you should create a user profile called the Guest. The functions defined for this branch will be applicable for a user of a different branch. Typically, this profile should have access to functions like inquiry into balances, etc. If this Guest profile is not created in a branch, a user not belonging to that branch will not be allowed to change branch to it.

The branch where the user profile is created is called the Home branch and the other branches are called Host branches.

2.6.2.3 User Belonging to AEOD Category

For such a user, the functions defined for the user profile where the profile created (the Home branch) will be applicable in every branch (Host branch).

2.6.2.4 User Transaction and Auth Limits

You cannot capture any transaction, if the transaction amount is greater than the maximum transaction amount. Also, you cannot authorise any transaction if the transaction amount is greater than the maximum authorization amount.

This validation is applicable only for UT transactions, Bulk transaction, adjustment transaction, light weight transaction and LEP – initial investment, top up, surrender and switch transaction types.

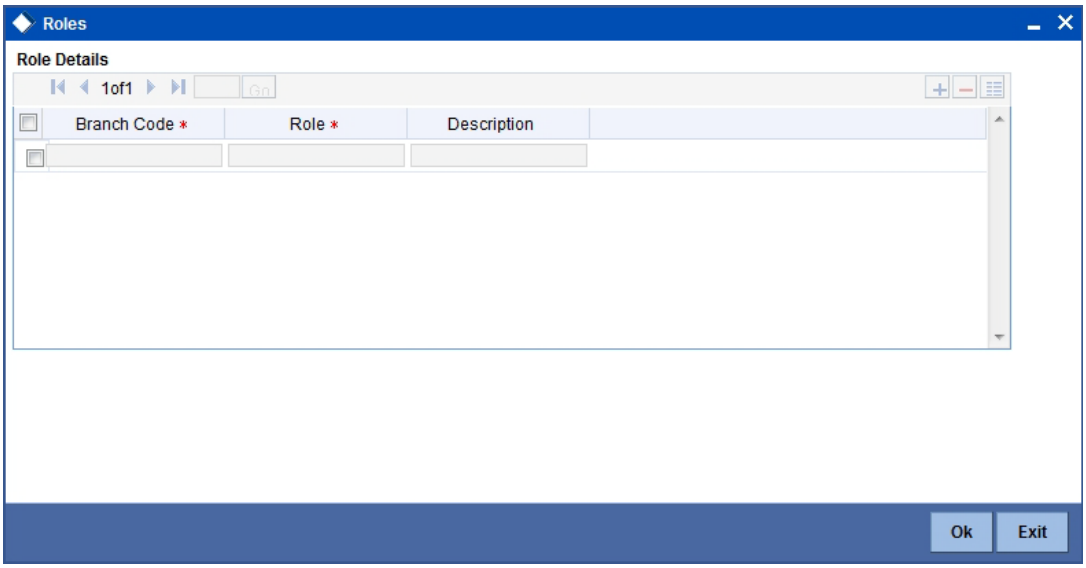
The validation will not be applied if there is no exchange rate currency maintained for the limit currency of the user and the transaction currency.

2.6.2.5 User Belonging to Customer Category

A user of this category can log on only to the branch where the profile is created.

2.6.3 Roles for User

Click 'Roles' button to attach the user profile you are defining to a role. The User Roles screen will be displayed.



You can attach a role to the user profile, to be operable at a specific branch. Select a branch from the adjoining option list.

A role profile could contain either back office (Fund Manager) functions or front office (Agency Branch) functions.

When you have selected the required roles, click the OK button to save your changes.

2.6.4 Functions for User

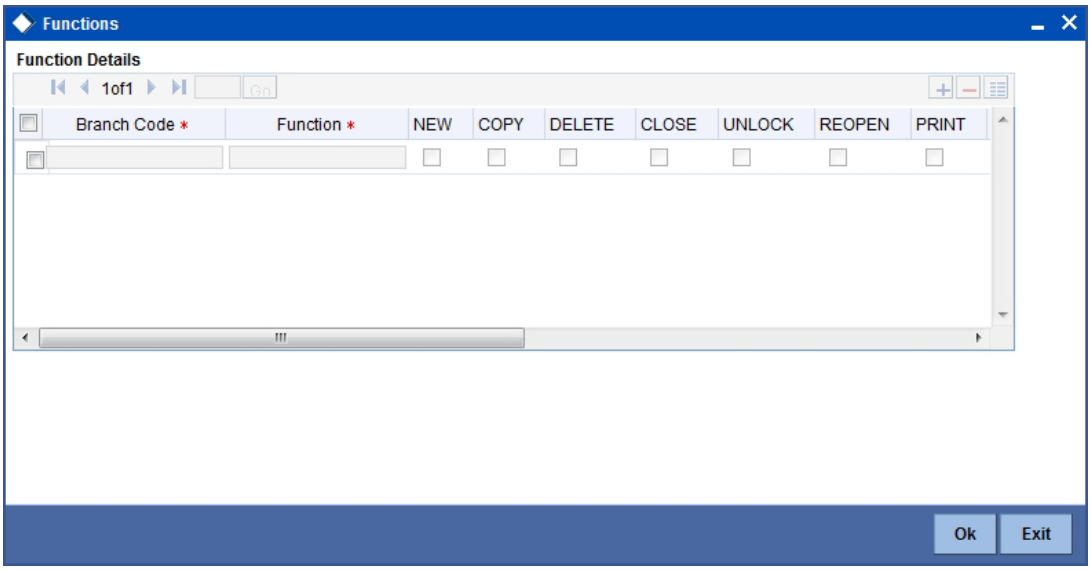
In addition to attaching a user profile to a role, you can give rights to individual functions. For a user profile to which no role is attached, you can give access to specific functions. If you have one of the following:

- Attached one or more roles to a user profile
- You have given access to individual functions to a profile to which roles are attached.

A user profile could be given access to either back office (Fund Manager) functions or front office (Agency Branch) functions, depending upon the tasks that the user has to perform within your organization.

The rights for Function IDs that figure in both the role and user specific functions will be applied as explained in the following example.

Click 'Functions' button in the User Profile Definition screen to give access to functions for the user profile you are defining. The User Functions screen will be displayed.



You can allow any of the following operations at record level for the user profile, in any function:

2.6.4.1 Static Screens

- New (Define a new record).
- Copy (Copy details of an existing record).
- Delete (Delete an existing record).
- Close (Close an existing record).
- Unlock (to amend an existing record).
- Reopen (Reopen an existing record).
- Print (Print the details of selected records).
- Authorize (Authorize any maintenance activity on a record).

2.6.4.2 Contracts and On-line Transaction Processing

1. View (to see the details of the contract).

2.6.4.3 Reports

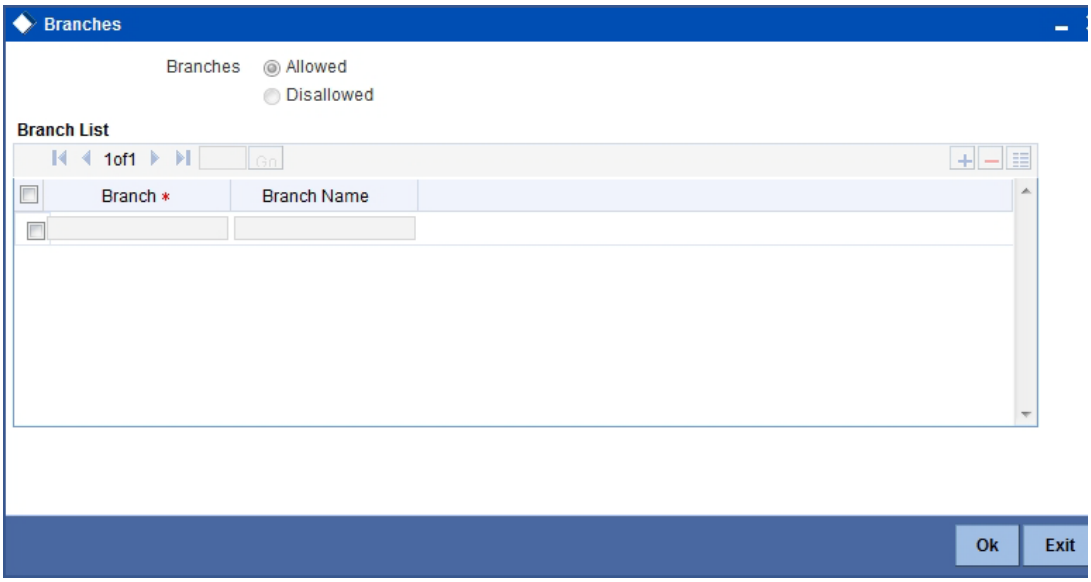
- Generate (to generate reports).
- View (view the reports).
- Print (print the reports).

To delete the access rights you have specified for a function, select the required Function ID row and check the Delete box to the left of the Function ID field.

To edit the access rights you have specified for a function, select the required Function ID row and check the Edit box to the left of the Delete field.

2.6.5 Branches for User

For Staff and End of Day users, you can specify the branches from which they can operate. Click 'Branches' button in the User Profile Definition screen to define the branches in which the user should be allowed to operate.



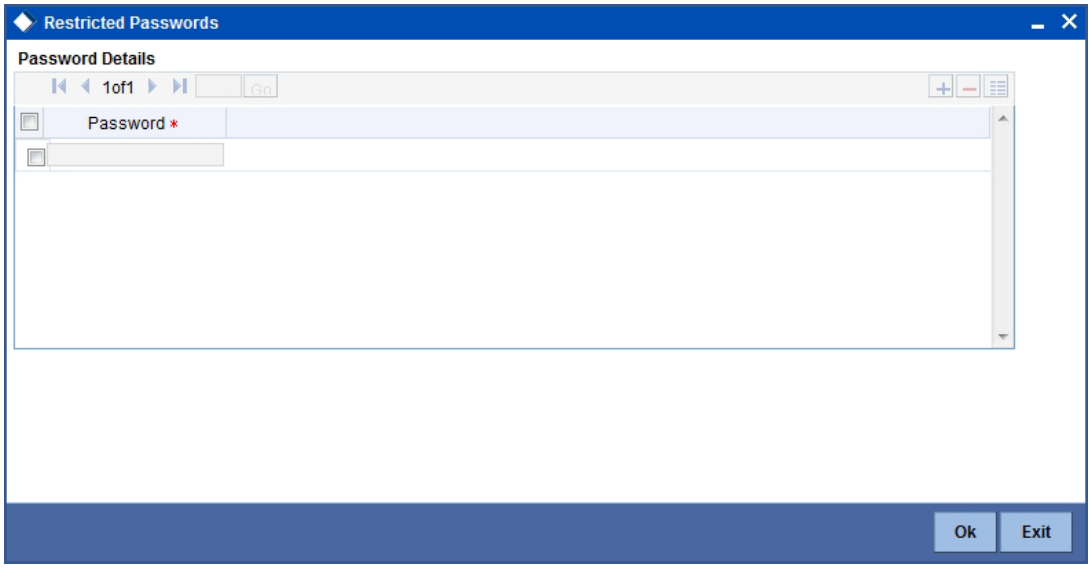
To prepare a list of branches from which the user is disallowed, choose the Disallowed option. Specify the branches that are disallowed for a user.

Similarly, to prepare a list of branches from which the user is allowed to operate, choose the Allowed option.

2.6.6 Restrictive Passwords for User

You can maintain a list of passwords that the user is most likely to use. For example, a user may tend to use the names of loved ones, the AMC or AMC branch, department, etc. as a password as they are easy to remember. This might be a security risk as it will be easy for another person to guess a password. To prevent this, you can maintain a list of passwords that the user should not use. This list of restrictive passwords will be checked before a password is accepted when the user is changing passwords. If the password entered by the user is listed, it will not be accepted.

Click ‘Restricted Passwords’ button in the User Profile Definition screen, left margin of the screen. The Restricted Passwords screen is opened, where you can define a list of such passwords.

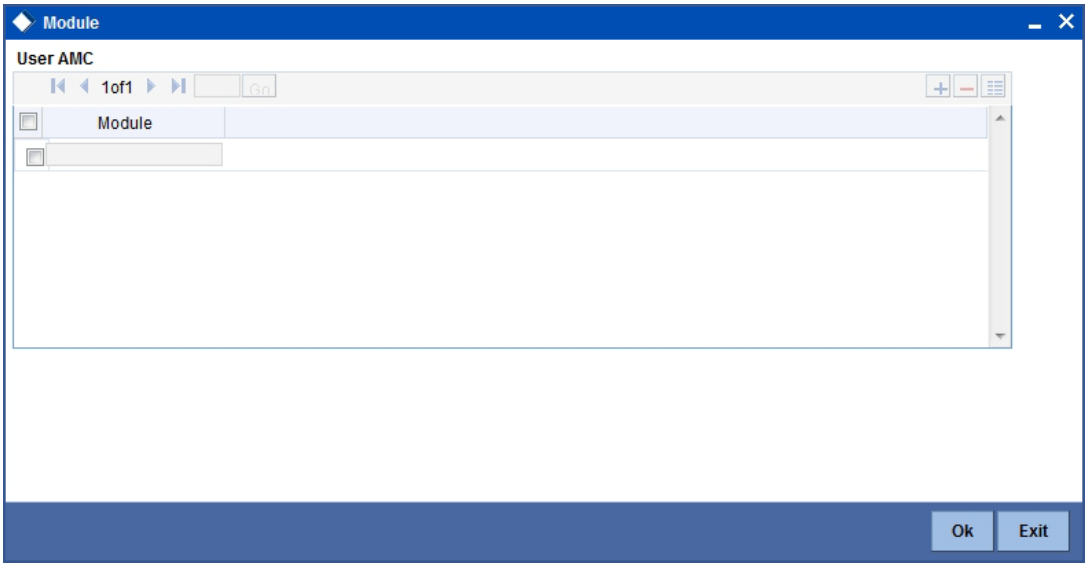


The user for whom you are defining the restrictive passwords cannot use the restrictive passwords defined in this screen.

2.6.7 Modules for User

You can restrict the user to operate only from certain Modules, or certain branches of an AMC. To define such a restrictive list of AMC’s or AMC branches, click ‘Module’ button in the left margin of the User Profile Definition screen.

The Module screen is displayed.

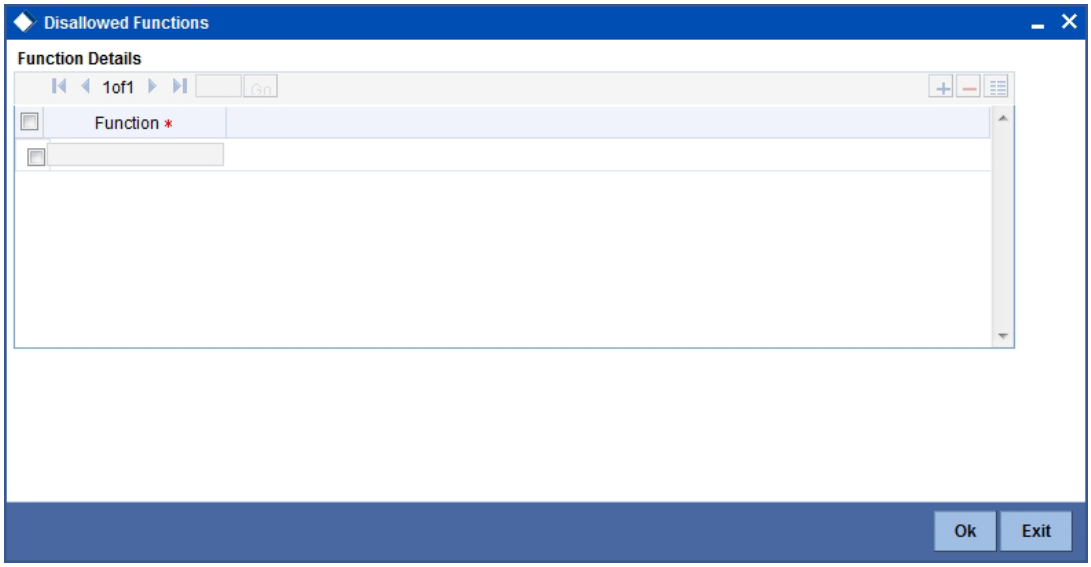


To allow the user to operate the system from a certain AMC, select it in the Available box, and move it to the Allowed box using the arrows. When you have selected the required AMC’s, click ‘Ok’ button to save your changes.

2.6.8 Disallowed Functions for Users

You can define a list of functions that the user is not allowed to operate, out of the functions list already associated with the user profile. To define such a restrictive list of functions, click 'Disallowed Functions' button in the left margin of the User Profile Definition screen.

The 'Disallowed Functions' screen is displayed. All the functions that are associated with the user profile are listed in the Available box.



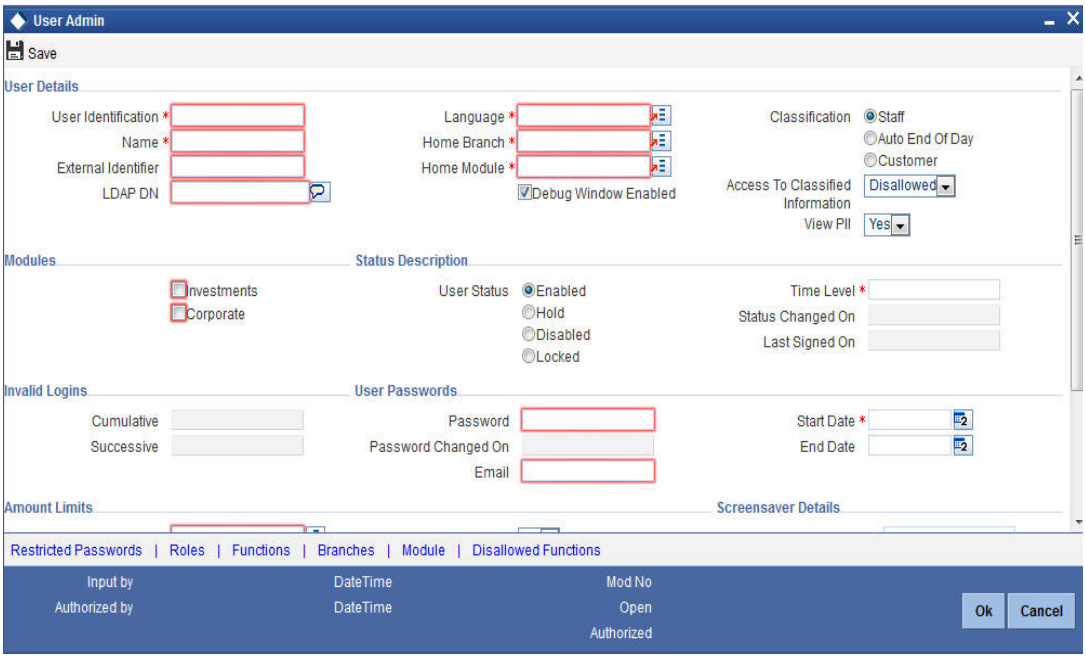
Click add icon. The system displays the available functions. Select the functions that you wish to disallow for the user.

2.6.9 Copying User Profile of Existing User

Often, you may have to create a user profile that closely resembles an existing one. In such a case, you can copy the existing profile on to the new one.

Click F7, input the User Identification and click F8. All the details pertaining to the User Identification specified are displayed. Choose the Copy button from the row of buttons at the topmost row of the screen. All the details of the profile except the User ID will be copied and displayed. Enter a unique User ID. You can change any of the details of the profile before saving it.

If you have retrieved an existing user profile and you want to copy it to a new user profile, click the Copy button in the topmost row of buttons in the screen. The Copy Information screen is opened, and you can specify the User ID for the new user profile.



All the details of the existing profile are copied onto the new user profile. Again, you can change any of the details of the profile before saving it.

2.6.10 Deleting User Profile

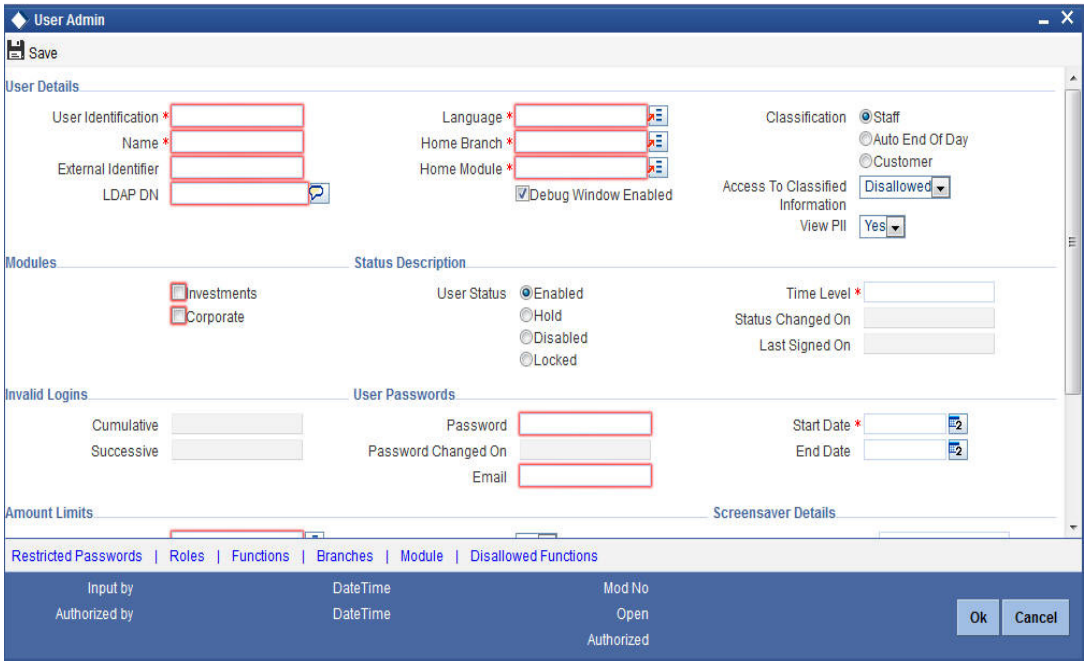
A user profile can be deleted only if the user is currently not logged on to the system.

To delete an existing user profile, retrieve the record of the user profile so that it is displayed in the main portion of the User Profile Definition screen. Then select the Delete button from the topmost row of buttons in the screen. If the user is logged in to the system, a warning message will be displayed and you cannot delete the profile.

If the user is not logged in, you will be prompted to confirm the deletion. The user profile will be deleted only if you confirm the deletion.

2.6.11 Retrieving User Profile in User Profile Definition screen

To retrieve a user profile that you have previously set up in the User Profile Definition screen, choose the Query button from the topmost row of buttons in the screen. The Query User screen is opened.



To retrieve a record:

- Press F7.
- Input the data.
- Press F8 to query the data.

In this screen, you can specify the parameters that will the system will use to locate the user profile in the database and retrieve it.

When the record is retrieved based on your search specifications, it is displayed in the User Definition screen.

2.6.12 Authorizing User Profile

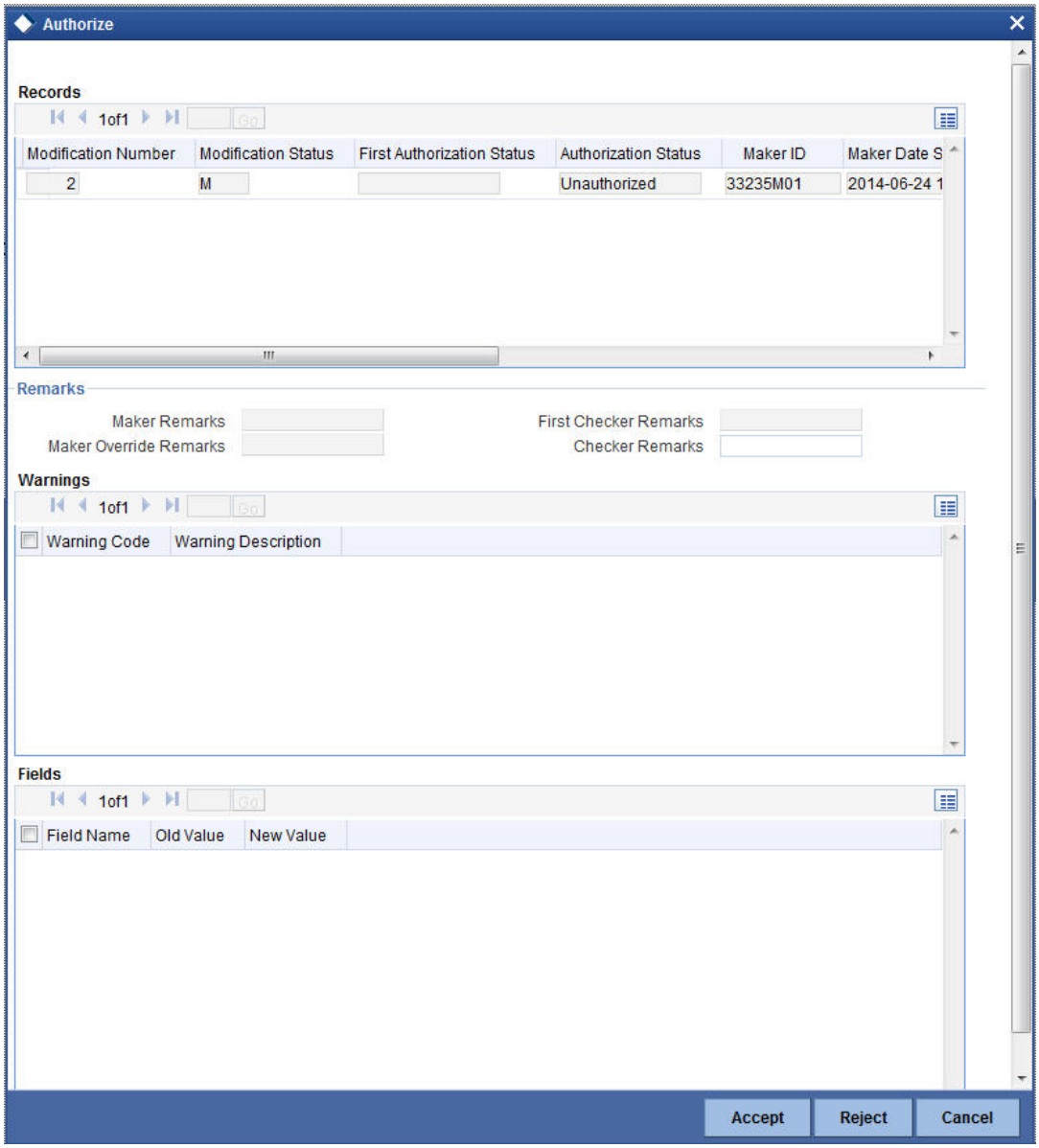
Before you link any users to a user, a user other than the one that defined it must authorize it.

To authorize a user profile:

- Retrieve the user profile record so that it is displayed in the User Definition screen.
- Click the Auth button from the topmost row of buttons in the screen. The Authorize User Admin screen is displayed. The details of each modification that was made to the record, in the sequence of occurrence is shown in this screen. For each modification, the following details are displayed:
  - The sequence number for the modification, in the Mod No. field.
  - The operation that resulted in the modification, the Action field.
  - The user that effected the modification, in the Input By field.
  - The time at which the modification occurred, in the Date Time field.
  - In the lower grid portion, the changed values for each modification are displayed.

- You can authorize any of the modified records, or all of them. Check the box in the Authorize field in the desired row, to mark it for authorization.

When you have marked the required modifications for authorization, click 'Ok' button to effect the authorization. The Maintenance Authorization Details screen is closed, and you are returned to the User Definition screen.



2.6.13 Editing User Profile

You can make changes to an authorized user profile as follows:

- Retrieve the user profile record so that it is displayed in the User Profile Definition screen.
- Click the Edit button from the topmost row of buttons in the screen. The record is now in readiness for modification.
- After making your changes, click the Save button from the topmost row of buttons in the screen to save your changes. The record is now an edited, unauthorized record. Another user must now authorize it for it to be effective again.
- Fields in User Profile Definition Screen

2.6.13.1 User Details Section

User Identification

Alphanumeric, Mandatory

Specify a unique identifier for the user profile.

Name

Alphanumeric, Mandatory

Specify the name of the user for the user profile.

External Identifier

Alphanumeric, optional

Specify the External Identifier. External user is an alternative name for user id where two users cannot have same External identifier.

Home Branch

Mandatory

Select the default branch from which the user profile will operate.

Lang

Mandatory

From the option list, select the default, preferred language for the user profile. The system displays Param Codes in the language assigned for the user, if they have been maintained in that language.

Home Module

Select the default module from which the user profile will operate.

Classification

Mandatory

Indicate the type of the user profile, whether the user is a staff user, customer user or an end of day operator (AEOD).

2.6.13.2 Modules Section

Mandatory

Indicate whether the user will operate corporate functions or investment functions in the system

2.6.13.3 User Status Section

The status of a user profile refers to whether or not it is enabled. A disabled user profile cannot operate on the system.

User Status

Mandatory

The status of the user profile in the system is shown in this field. By default, every user profile is created as an enabled profile. The status could be:

- Enabled – the profile is enabled and active in the system
- Disabled – it cannot be used to operate in the system
- Hold – the status is on hold in the system.

Status Changed On

Display Only

The most recent date on which the status of the user profile was changed is displayed here.

Time Level

Display Only

Last Signed On

Display Only

The most recent date on which the user logged in to the system is displayed here.

2.6.13.4 Password Section

Password

Alphanumeric, Mandatory

Specify the password using which the user will log in to the system.

At the time of setting up the Oracle FLEXCUBE Investor Servicing, the number of repeated successive parameters allowed in a password will be indicated.

For example, if the number of repeated successive parameters allowed in a password has been set as '2', then the user password can have a character repeating only twice. Suppose, if the number of repeated successive parameters has been specified as 2, a user password like AAA777 will be invalid. A valid password would be AA77.

Password Changed On

Display Only

The most recent date on which the password was changed is displayed here. When you are entering a new record, this field is blank and locked.

Start Date

Date format, Optional

Specify the date on and following which the password is valid.

End Date

Date Format, Optional

Specify the date up to which the password is valid.

Email

Mandatory when Auto Generation of Password is Yes.

System generates a password with respect to the predefined parameter set up in the SMS parameter Maintenance and password is send to the respective Email Id mentioned in the field.

Optional when Auto Generation of Password is No.

System does not generate a password; user has to get the password from User Admin screen.

2.6.13.5 Amounts Limit Section

Txn Amount

Numeric, Mandatory

Specify the maximum amount value that the user can specify while entering a transaction request from an investor.

Auth Amount

Numeric, Mandatory

Specify the maximum amount value of an investor transaction that the user can authorize.

Override Amount

Numeric, Mandatory

Specify the maximum amount value that the user can override while entering a transaction request from an investor.

2.6.13.6 Invalid Logins Section

Successive

Numeric, Optional

Specify the number of successive invalid login attempts (in a single session) after which the user ID will be disabled for this profile.

Cumulative

Numeric, Optional

Specify the number of successive invalid login attempts (spread across different sessions) after which the user ID will be disabled for this profile.

Status Bar Information

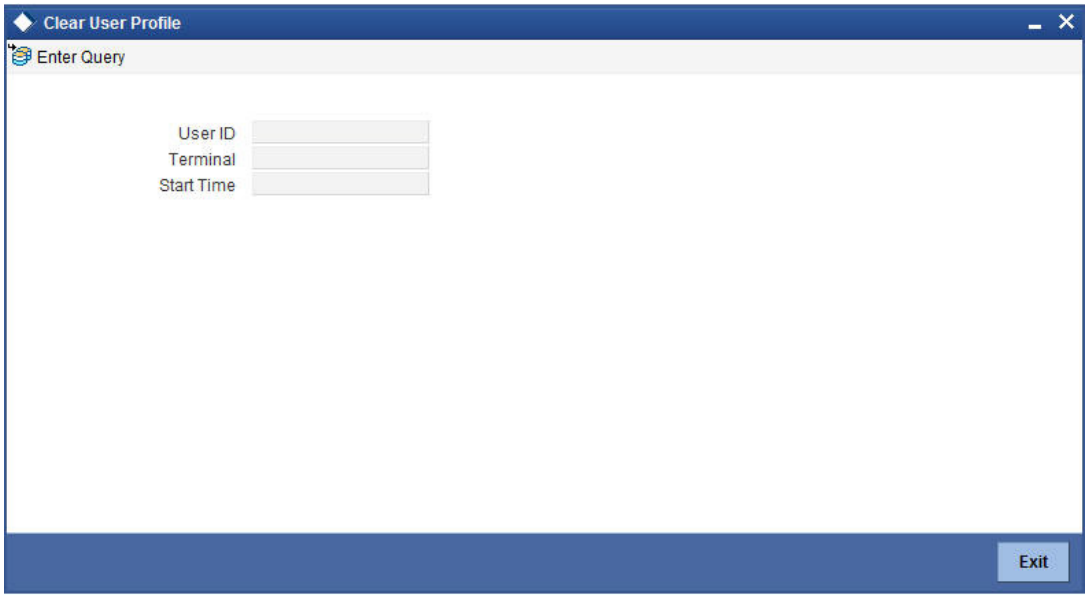
In this section, the following details are displayed for any user profile record:

- The user that has created the user profile, in the Input By field.
- The date and time of user profile creation, in the Date Time field.
- The user that has authorized the user profile, in the Authorized By field.
- The date and time of user profile authorization, in the Date Time field.
- The serial sequence number of the most recent modification of the user profile, in the Mod No field.
- The authorization status of the record, in the Authorize field.
- The open status of the record, in the Open field.

2.7 Clearing User that has Exited System Abnormally

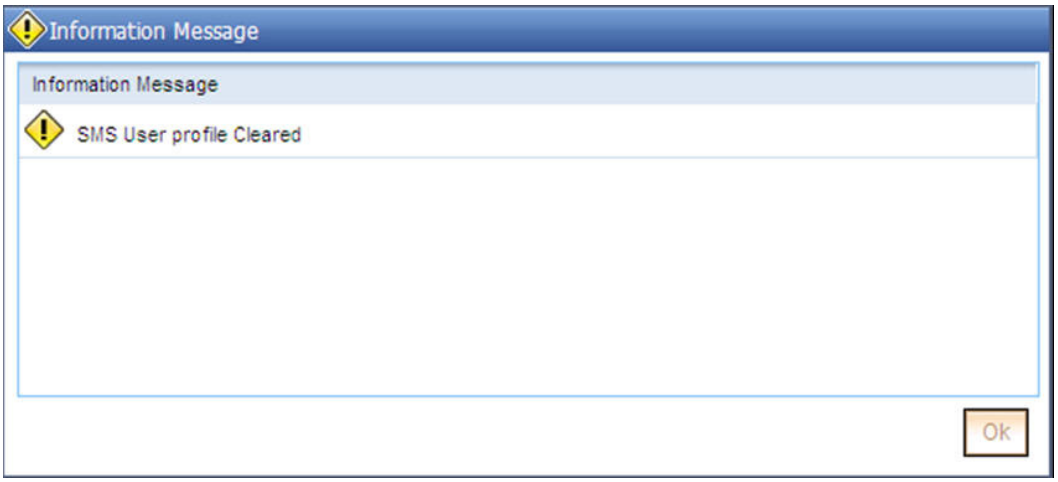
If a user exits the system abnormally, the administrative users can clear the logged in user profile so that the user can log in normally again

To clear a user, log in to the system as an administrative user, and type ‘SMDCLUSR’ in the field at the top right corner of the Application tool bar and click the adjoining arrow. The ‘Clear User Profile’ screen is displayed.



In this screen, press F7 and select the User Id from the adjoining option list which displays the users logged in currently. After specifying the user id to be cleared, press F8. Upon pressing F8, system displays the terminal and start time information.

Now click on the unlock icon from the toolbar menu and then click on save icon. The system will clear the selected user id and will display the following message:



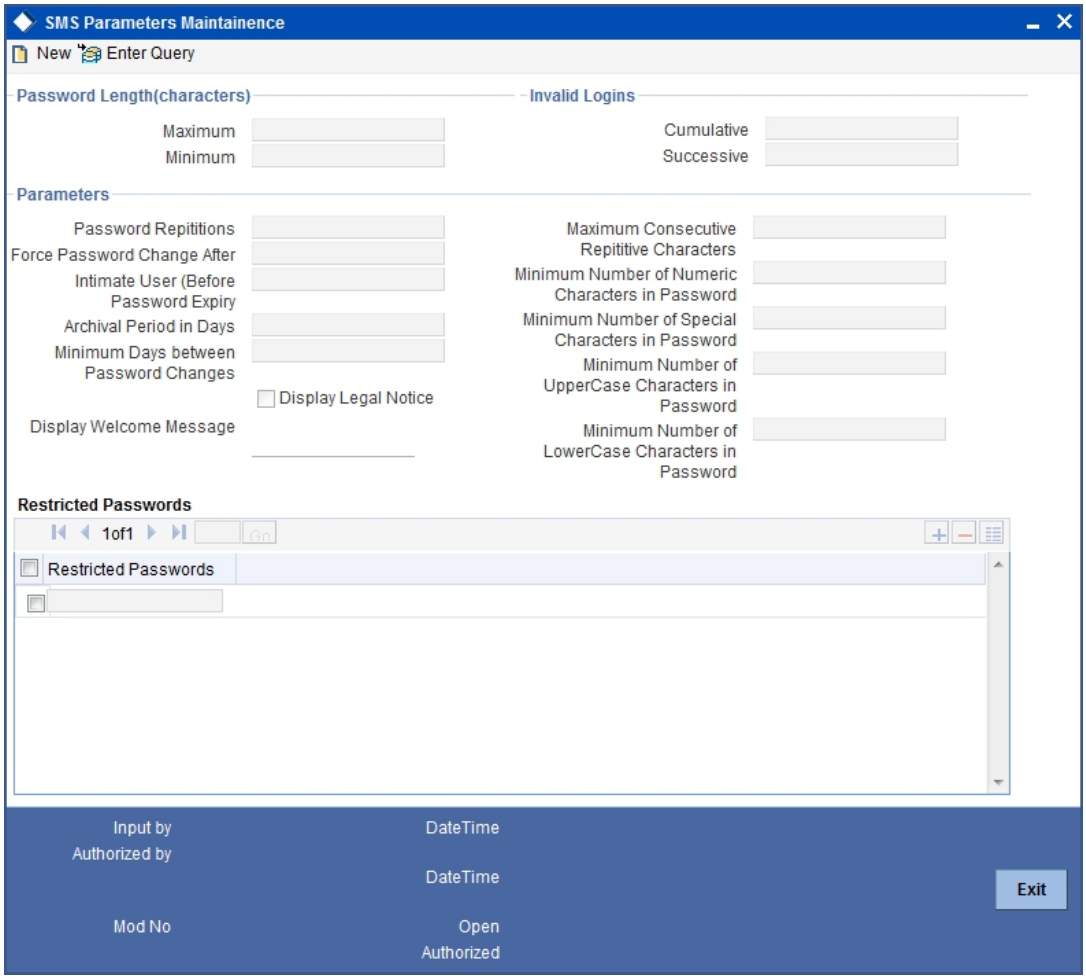
Click on OK to confirm..

To clear a user, check ‘Clear’ in the required row, and then click ‘Clear’ button.

2.8 Setting up SMS Parameters

You can set up certain parameters related to invalid logins and passwords using the ‘SMS Parameters Maintenance’ screen. You can invoke the ‘SMS Parameters Maintenance’ screen

by typing ‘SMDPARAM’ in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button. The screen is displayed below:



2.8.1 Fields in SMS Parameters Maintenance Screen

2.8.1.1 Password Length (characters)

Maximum

Numeric; Optional

Indicate the maximum number of characters to be used for a password. The number of characters in a user password is not allowed to exceed the maximum length that you specify here.

The maximum length of password defaults to 15.

Minimum

Numeric; Optional

Indicate the minimum number of characters to be used for a password. The number of characters in a user password is not allowed to fall below the minimum length that you specify here.

The minimum length of password defaults to 8. The minimum length that you specify must not exceed the maximum length that you have specified.

2.8.1.2 Invalid Logins

Cumulative

Numeric, Optional

Specify the allowable number of cumulative invalid attempts made during the course of a day, as well as the allowable number of consecutive or successive invalid attempts made at a time. In either case, if the number of invalid attempts exceeds the stipulated number, the user ID is disabled.

Successive

Numeric, Optional

Specify the allowable number of times an invalid login attempt is made by a user. Each user accesses the system through a unique User ID and password. While logging on to the system, if either the User ID or the Password is wrong, it amounts to an invalid login attempt. If the number of invalid attempts exceeds the stipulated number, the user ID is disabled.

Note

When authentication of credentials is unsuccessful due to an incorrect user ID, then the user id will not be logged in the audit logs. In case the user id is correct and the password is wrong, the attempt is logged in the audit log and the successive and cumulative failure count is incremented. When the user id and password are correct, this is logged into the audit logs.

2.8.1.3 Parameters

Password Repetitions

Numeric, Optional

Specify the number of previous passwords that cannot be set as the new current password, when a password change occurs.

Force Password Change after

Numeric, Optional

Specify the number of calendar days for which the password should be valid. After the specified number of days has, it is no longer a valid password and the user will be forced to change the password.

Minimum Days between Password Changes

Numeric, Optional

Specify the minimum number of calendar days that must elapse between two password changes. After a user has changed the user password, it cannot be changed again until the minimum number of days you specify here have elapsed.

Display Welcome Message

Optional

Check this option if you want to display welcome message when the login screen is launched.

Welcome Text Message

Alphanumeric; Conditional

If you have selected the ‘Display Welcome Message’ option, then specify the welcome text message to be displayed on launching the login screen,

Intimate Users (before password expiry)

Numeric, Optional

Specify the number of working days before password expiry that a warning is to be issued to the user. When the user logs into the system (the stipulated number of days before the expiry date of the password), a warning message will continue to be displayed till the password expires or till the user changes it.

Maximum Consecutive Repetitive Characters

Numeric, Optional

Define the maximum number of allowable repetitive characters occurring consecutively, in a user password. This specification is validated whenever a user changes the user password.

Minimum Number of Numeric Characters in Password

Numeric, Optional

Define the minimum number of numeric characters allowed in a password. The system validates the password at the time of creating a User ID in User admin screen and at the time when a user chooses to change his password.

- .Minimum No of Special Characters = 1

Minimum Number of Special Characters in Password

Numeric, Optional

Define the minimum number of special characters allowed in a password. The system validates the password at the time of creating a User ID in User admin screen and at the time when a user chooses to change his password.

- Minimum No of Special Characters = 1

Minimum Number of Upper Case Characters in Password

Numeric, Optional

You can define the minimum number of upper case characters allowed in a user password. The allowed upper case characters are from the US-ASCII character set only. The system validates the password at the time of creating a User ID in User admin screen and at the time when a user chooses to change his password.

If you do not specify the limits, the following default values will be used:

- Minimum No of Upper Case Characters = 1
- Maximum No of Numeric Characters = Maximum Password Length

Minimum Number of Lower Case Characters in Password

Numeric, Optional

You can define the minimum number of lowercase characters allowed in a user password. The allowed lower case characters are from the US-ASCII character set only. The system validates the password at the time of creating a User ID in User admin screen and at the time when a user chooses to change his password.

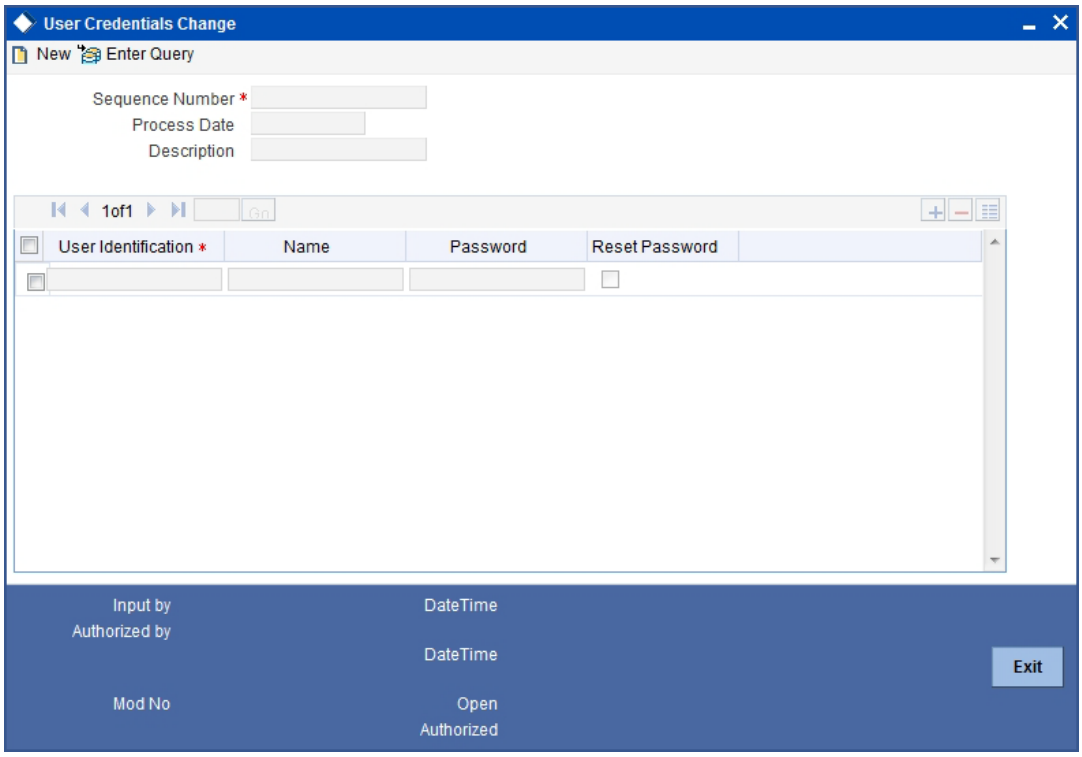
If you do not specify the limits, the following default values will be used:

- Minimum No of Lower Case Characters = 1
- Maximum No of Numeric Characters = Maximum Password Length

2.9 User Details Modification in Bulk

You can change or reset user passwords in bulk if you have the system admin rights. After modification of the user list, click 'Save'. The modified user list will be stored in a temporary table. The lists of users which are modified and mapped with a unique sequence number will not be available until the particular sequence number is authorized. When the particular sequence number is authorized those user details will be changed and updated.

You can invoke this screen by typing 'SMDCHPWD' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



In this screen, the following information is to be provided.

Sequence Number

Alphanumeric, Mandatory

Click on 'New' icon to generate a new 'Sequence Number'.

Process Date

Date Format

Select a date by clicking on the calendar icon beside the field. This field is generally useful for querying purpose.

Description

Alphanumeric, Optional

Provide a description of what modification is being done on selected user ids.

User Id

Alphanumeric, Mandatory

Select the User Id to be changed from the option list provided.

Name

Alphanumeric, Optional

Name of the user specific to the selected user id will be displayed in this field.

Password

Optional

Password of the selected user id will be displayed here. This field will be editable only if the 'Auto Generation Required' option is not selected at the application level. If the 'Auto Generation Required' option is checked, the password will be auto generated by the application.

Reset Password

Optional

Select this checkbox to reset the password in case of user ids where password needs to be auto generated.

2.10 Modules

Typically, in an AMC, an installation of Oracle FLEXCUBE Investor Servicing installs the following components:

- Fund Manager
- Agency Branch

In a network scenario, the following situations are also possible:

- A single AMC with a single installation may have two or more "instances" of each component, or all components, as necessary.
- A multi-AMC situation where a number of AMC's are networked and each has one or more installation of all components.

In either case, each installation of any or all of the components may have a different instance, or schema. However, for the purpose of multi-networking and enabling a user to log in to the system with a single user ID from any component, a single Security Management System database is necessary that contains the repository of all users in all the different instances.

Each instance of the installation, in a multi-networked situation, is referred to a Module.

A Module, therefore, is an instance of either one of the components, connecting to a single SMS database.

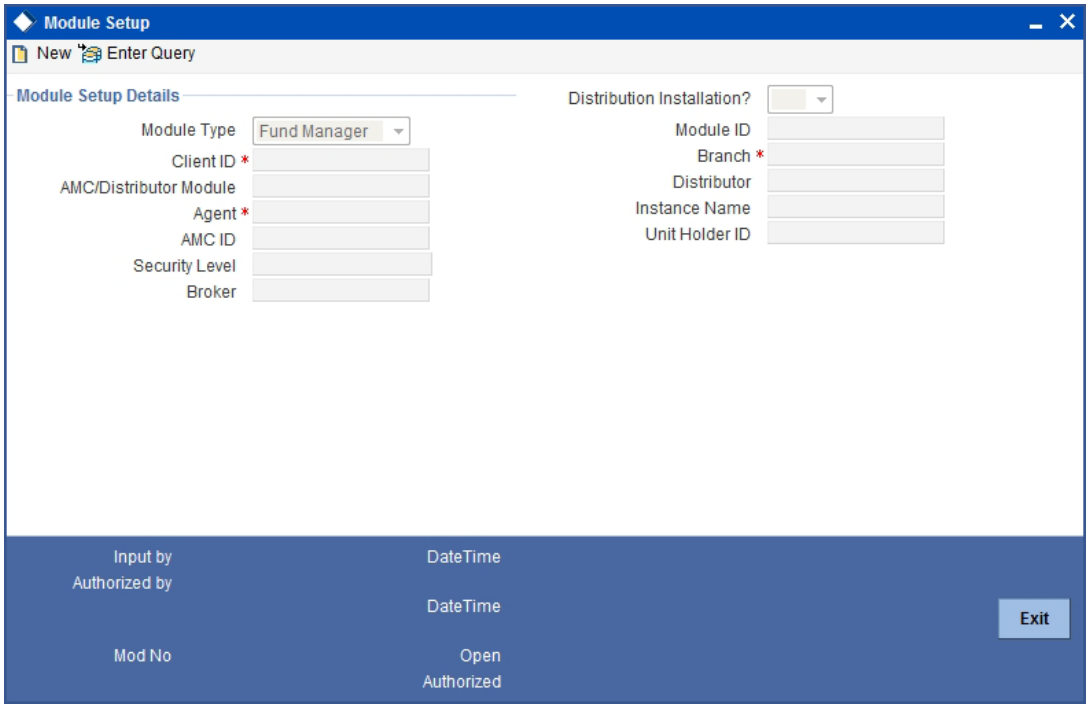
2.10.1 Setting up Modules

At the time of installation, the installation process sets up the Fund Manager module in the system, with a default agent and branch code.

Subsequently, the Sysadmin User must set up the Agency Branch module.

Subsequently, if any new agency branch modules need to be created, the Sysadmin User can create them using the 'Module Setup' screen. You can invoke this screen by typing

'SMDMODUL' in the field at the top right corner of the Application tool bar and click the adjoining arrow. The screen is displayed below:



To set up a module, proceed in the following manner:

- Click on the Module Profile button in the Restricted Access screen. The system displays the Module Profile Maintenance screen. The profile of the logged-in module is displayed. Click on the Add button to specify a new module. To make changes to the logged-in module, click the Amend button.
- Proceed to specify all the details of the Module that you want to set up, in the following sequence:
  - The ID of the Module, in the Module ID field. This must be unique, and if any duplicates are detected by the system, a warning message is displayed.
  - The connect string that identifies the instance for the module in the system registry, in the Connect String field. The connect string must contain the DSN name, user name and the password.
  - The agent and branch combination that will together be created as a Module, in the Agent Code and Branch Code fields. You can use the drop down lists to make your choice.
  - The type of module you are setting up, in the Module Type field. This could be Fund Manager or Agency Branch.
  - The ID of the client where the module is being created, in the Client ID field.
  - If the module is to be a single entity agency branch, consisting of just one broker or unit holder, specify the corresponding ID of the entity, in the Broker or Unit Holder fields, as necessary.
  - Click save icon to save your user profile record. The system confirms the saving of the record.

The record is saved into the SMS database.

2.10.2 Operations on Module Record

After you have set up a module, you must have another user authorize it so that it would be effective in the system.

Before the module is authorized, you can edit its details as many times as necessary. You can also delete it before it is authorized.

After authorization, you can only make changes to any of the details through an amendment.

The Module Profile Maintenance screen can be used for the following operations on modules:

- Retrieval for viewing
- Editing unauthorized modules
- Deleting unauthorized modules
- Authorizing modules
- Amending authorized modules.

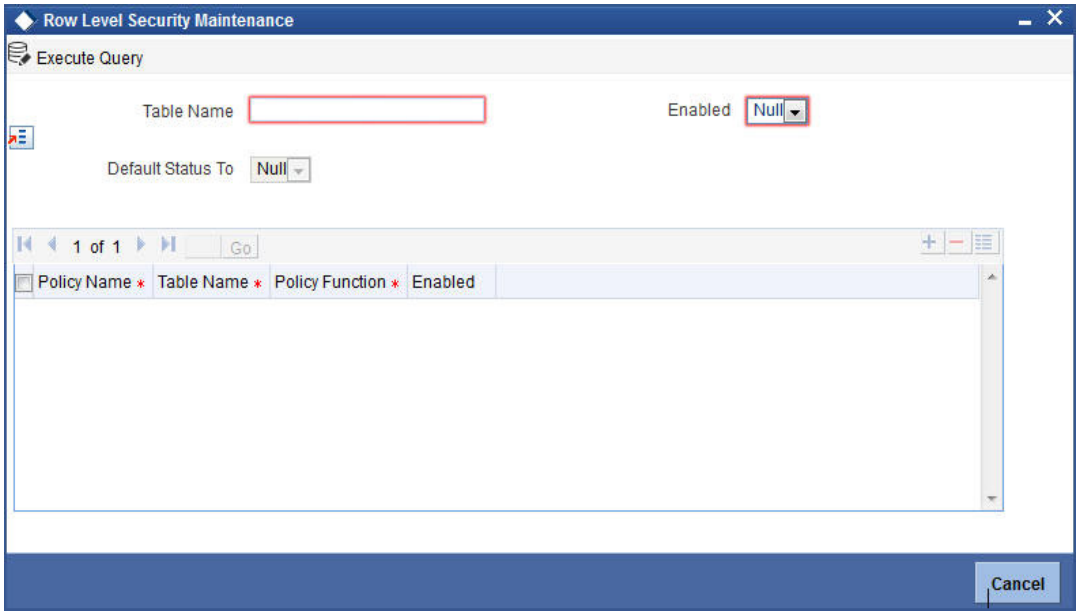
2.11 Row Level Security Maintenance

This section contains the following topics:

- Section 2.11.1, "Invoking Row Level Security Maintenance Screen"

2.11.1 Invoking Row Level Security Maintenance Screen

You can enable or disable RLS policy using 'Row Level Security Maintenance' screen. You can invoke this screen by typing 'UTDRLSMT' in the field at the top right corner of the Application tool bar and click the adjoining arrow.



You can specify the following details:

Table Name

Alphanumeric; 30 Characters; Optional

Specify the table name. Alternatively, you can select table name from the option list. The list displays all valid table name maintained in the system.

Enabled

Optional

Select if row level security to be enabled or not from the drop-down list. The list displays the following values:

- Yes
- No

Default Status To

Optional

Select the defaulted status from the drop-down list. The list displays the following values:

- Yes
- No

Click ‘Execute Query’ button to display the following details:

- Policy Name
- Table name
- Policy Function

Enabled

Optional

Select if RLS policies to be enabled or not from the drop-down list. The list displays the following values:

- Yes
- No

By default all the policy will be disabled.

Note

You can create new maintenance but will be restricted to delete or amend existing/ created policies.

On enabling the policy rule, the system will create new RLS policy. On disabling the system will drop the RLS policy.

Note

In case of enabling or disabling RLS policy, you should either enable it or disable it all. In case of partial enabling, the system behaviour could differ.

---

3. Ensuring Security for Agency Branch

3.1 Introduction

In any financial environment, security of information is of paramount importance. Access to information must be made available in a carefully monitored manner. Controlling and maintaining these aspects also includes management of the people (or users) who will process this information on a day to day basis. Therefore, an efficient Security Management System is an important factor that will determine the strength and stability of a financial system.

This chapter takes you through the Security Maintenance features of the Oracle FLEXCUBE system. You will learn how to use the security features in the system to suit your requirements and customize them for your environment.

This chapter is intended for the following persons in your bank or AMC:

Person	Operation
Oracle FLEXCUBE Implementers	To set up the initial start-up parameters in the individual client workstations. To set up security management parameters for the AMC or AMC branch.
SMS Administrator for the Bank/ AMC	To set the SMS AMC or AMC branch parameters. To identify the Branch level SMS Administrators.
SMS Administrator for the Branch	To create User and Role profiles for the branches of your AMC. Will also grant access to the various functions to the Users.
A Oracle FLEX-CUBE user	Any user of Oracle FLEXCUBE whose activities are traced by the Security Management System.

3.2 Security Management

In Oracle FLEXCUBE, you can ensure security management at all levels in any kind of environment. This is due to a combination of the following features:

- User-level Access Control
- Business function-level Access Control
- Operation-level Access Control

Simply translated, this means that a person within your environment can:

- Only access the system as an authorized user.
- Only access certain allowed functions within the system.
- Only perform certain allowed operations on the function for which access is allowed.

3.3 Some Important Terms

Before you operate the security management system of your Oracle FLEXCUBE installation, you must understand some important terms that you will encounter during the process.

3.3.1 System Administrators

Typically, at the time of installation, two users are created by default in the system database. These two users are the system administrators.

The system administrators subsequently create all users and user roles in the system, enabled by the logging in of the control clerks.

The system administrator user profiles would be typically created to enable the security managers in your bank or AMC, to log in to the system.

3.3.2 Functions

A function is any operation related to business maintenance or processing in the system. Most typically, each menu item appearing in the main menu could be thought of as a function. For a user, you can control access to different functions in the system.

Any functions related to the Fund Manager component can be thought of as back office functions, and any functions related to the Agency Branch could be thought of as front office components.

The functions are made available by the Oracle FLEXCUBE implementers, at the time of installation.

3.3.3 User Profile

Each user who will use the system is given a unique profile in the database. This profile is known as a user profile.

The profile of a user contains the User ID, the password and the functions to which the user has access. A user can be assigned access to either back office (Fund Manager) functions, or front office (Agency Branch) functions, depending upon the tasks that the user must perform in your organization.

3.3.4 Roles

It is likely that users working in the same department at the same level of hierarchy need to have similar user profiles. In such cases, you can define a Role Profile, which includes access rights to the functions that are common to a group of users. A user can be linked to a Role Profile by which you give the user access rights to all the functions in the Role Profile.

A role profile could contain either back office (Fund Manager) functions or front office (Agency Branch) functions.

3.4 Other Features of Security Management System

3.4.1 Restricted Number of Unsuccessful Attempts

You can define the maximum number of unsuccessful attempts after which a User ID should be disabled. When a User ID has been disabled, the system administrators can enable it. The password of a user can be made applicable only for a fixed period. This forces the user to change the password at regular intervals thus reducing security risks. Further, you can define passwords that could be commonly used by a user as Restrictive Passwords at the user, user role and bank level. A user cannot use any password that is listed as a Restrictive Password at any of these levels.

3.4.2 Restricted Access to Branches

You can indicate the branches from where a user can operate. Click on the User Branch Restrictions button in the User Profile Definition screen to define the branches from where a user can operate.

3.4.3 Restricted Access to AMC Branches

For mutual fund account customers, you can indicate the branches of the AMC from where a user can operate. Click on the AMC button in the User Profile Definition screen to define the branches of the AMC from where a user can be allowed to operate.

3.4.4 Restricted Access to Unit Holder Information

In FCIS, you can view all details related to any unit holder (UH) account or CIF customer account at any point of time using the Consolidated Inquiry query. It is therefore necessary to ensure that users' (agents) access is restricted only to data they require. This is possible by defining groups and mapping users to these groups so as to make certain the users view data pertaining only to the groups and agency branches they are mapped to.

Assume the following:

Agency Branches	**HK (Hong Kong), TA (Taiwan) and LUX (Luxembourg)**
Users	PB, JC and JY
Existing Groups in the agency branches	IS (Intermediary Sales) & DS (Direct Sales)

Let us consider the following examples to see the data available to a user, based on his group and agency branch mappings, when he queries a unit holder in the Consolidated Inquiry screen:

Case 1

Assume a user 'PB' is mapped to the agency branch 'HK' and the groups 'DS' and 'IS'. In such a case, the user 'PB' is restricted to accessing details of only 'DS' and 'IS' unit holders maintained in the 'HK' agency branch (i.e. HK-DS and HK-IS). He cannot access unit holder details maintained in' LUX' or 'TA' agency branches.

Case 2

Assume a user 'JC' is mapped only to the agency branch TA and to the groups 'IS' and 'DS'. He can access all details of unit holders belonging to the two groups (TA-DS and TA-IS). However, he cannot access unit holder details maintained in 'LUX' or 'HK' agency branches.

Case 3

Assume a user 'JY' is mapped to the agency branches 'HK' and 'TA' and to the groups 'IS' and 'DS'. This user can access unit holder details for the two groups in both the agency branches (i.e. HK-IS, HK-DS, TA-IS, TA-DS). However, he cannot access unit holder details maintained in the 'LUX' agency branch.

In the case of a UH, the system assigns the group of the UH's default intermediary agent as the group of the UH. Therefore, when a user queries a UH in the Consolidated Inquiry screen, information is made available only if:

- The user is mapped to the agency branch where the UH was created and

- The user is mapped to the group to which the UH's default intermediary agent belongs

For instance, if the default intermediary agent of a unit holder UH1 in the 'HK' agency branch is 'CITI' and 'CITI' belongs to the group 'IS', the user 'PB' (specified earlier) would have access to details regarding UH1.

But in both the following cases the user 'PB' would not be able to access the details for UH1:

- The unit holder UH1 had been created in the agency branch 'LUX'
- The default intermediary agent 'CITI' belonged to a group called 'TW'

The process of such data segregation (creating restrictions on data access for different users) is explained below:

3.4.5 All Activities Tracked

An extensive log is kept of all the activities on the system. You can generate reports on the usage of the system anytime. These reports give details of unsuccessful attempts at accessing the system along with the nature of these attempts. It could be an unauthorized user attempting to use the system, an authorized user trying to run a function without proper access rights, etc.

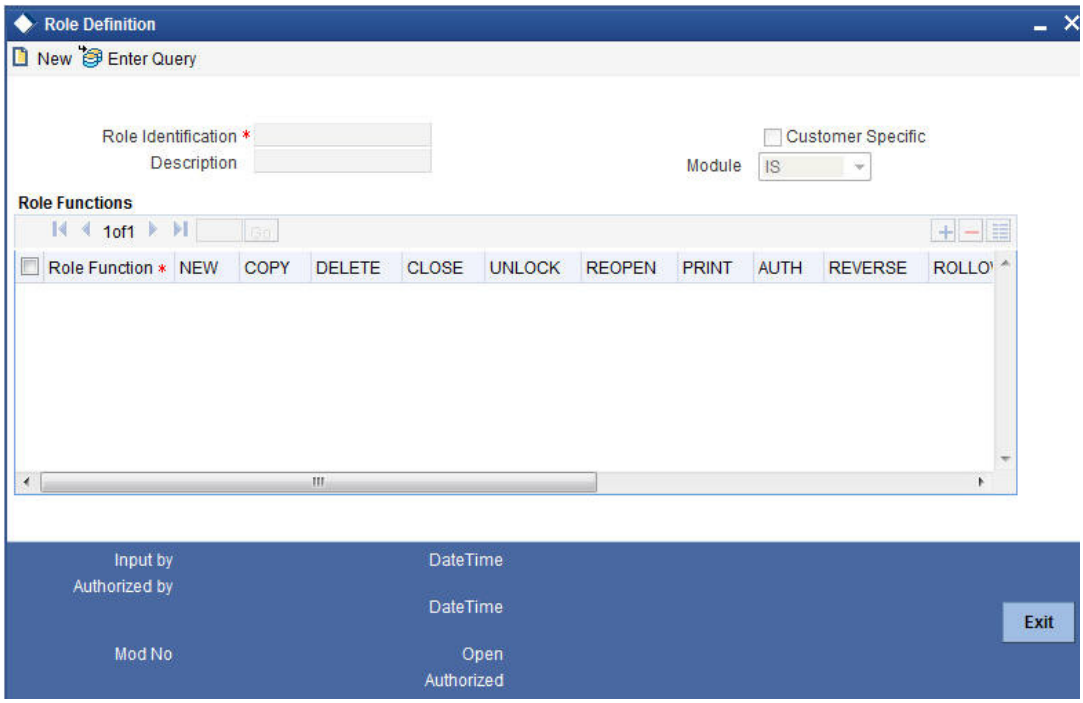
3.5 Defining User Role

To recall, a Role Profile includes access rights to the functions that are common to a group of users.

After you have a defined a Role Profile, you can link any user to it, thereby giving the linked user access rights to all the functions included in the Role Profile.

3.5.1 Procedure for Defining Role Profiles

Role profiles are defined in the Role Definition screen. You can access the Role Definition screen by typing 'SMDROLDF' in the field at the top right corner of the Application tool bar and click the adjoining arrow. The screen is displayed below:



3.5.2 Fields in Role Definition Screen

Role Identification

Alphanumeric, Mandatory

Specify a unique identifier for the role profile.

Description

Alphanumeric, Mandatory

Key in some text that describes and qualifies the role profile, and is indicative of its characteristics.

Customer Specific

Optional

Check this box to indicate that the role profile has been set up for a specific customer of your AMC or AMC branch who might access the system from a remote terminal to inquire about their transactions or investor accounts.

Module

Optional

Select the default module for users linked to the role profile.

In this screen, you define a role profile as follows:

1. Click the Add button in the topmost row of buttons in the Role Definition screen. The screen is now in readiness for you to enter a new record.
2. Assign a unique identifier (ID) for the role, and a description.
3. You can then indicate that the role is to be deemed as specific to a customer, by checking the Customer Specific box.
4. You can also link it to a module in the system, either the Corporate Module or the Investment Module.
5. Then, you must indicate the functions that the role profile has access to.

You can allow any of the following operations at record level for the role profile in any function:

3.5.2.1 Static Tables

- NEW (Define a new record)
- COPY(Copy details of an existing record)
- DELETE (Delete an existing record)
- CLOSE (Close an existing record)
- UNLOCK (to amend an existing record)
- REOPEN (Reopen an existing record)
- PRINT(Print the details of selected records)
- AUTH (Authorize any maintenance activity on a record)
- REVERSE
- ROLLOVER
- CONFIRM
- LIQUIDATE
- HOLD
- TEMPLATE

- VIEW
- GENERATE

3.5.2.2 Contracts And On-Line Transaction Processing

- VIEW (to see the details of the contract)

3.5.2.3 Reports

- GENERATE (to generate reports)
- VIEW (view the reports)
- PRINT (print the reports)

To delete the access rights you have specified for a function, select the required Function ID row and check the Delete box at the extreme right end of the row.

To edit the access rights you have specified for a function, select the required Function ID row and check the Edit box at the extreme right end of the row.

3.5.3 Classifying Role Profile

By default, a Role Profile you define will be for the users who are employees of your AMC or AMC branch. You can indicate that the profile is for customers who might login from remote terminals to inquire on their transactions and balances.

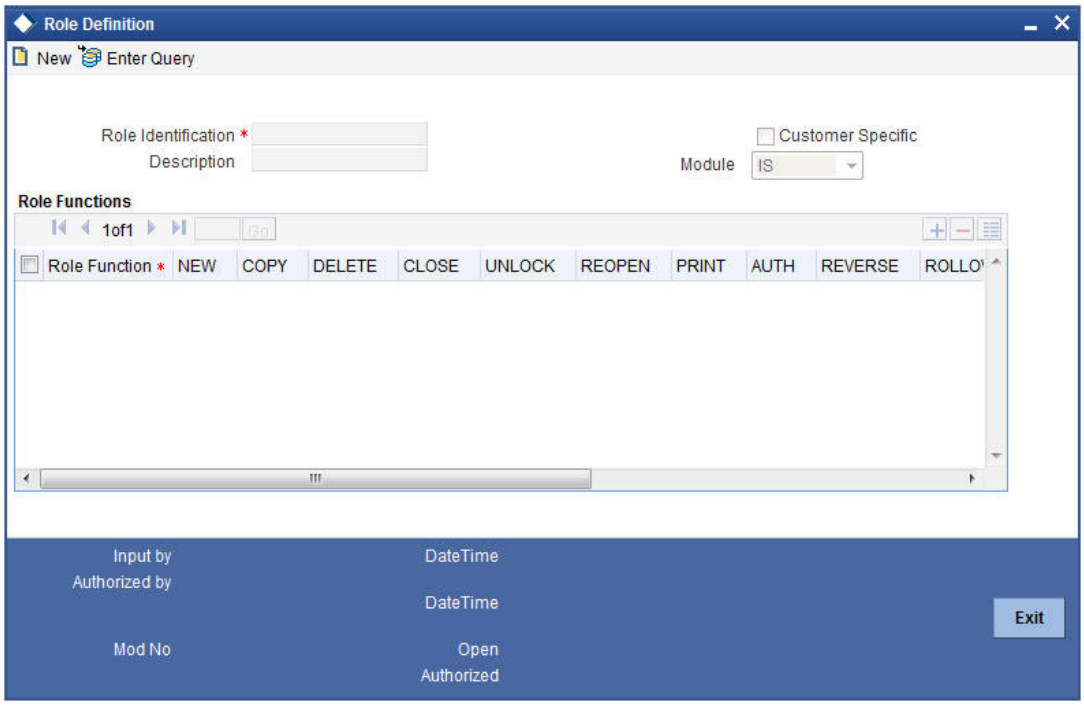
3.5.4 Copying Role Profile

Often, you may have to create a Role Profile that closely resembles an existing one. In such a case, you can copy the existing profile on to the new one.

Choose the Copy button from the row of buttons at the topmost row of the screen. A list of existing role profiles will be displayed. Click on the one you want to copy. All the details of the profile except the Role ID will be copied and displayed. Enter a unique Role ID. You can change any of the details of the profile before saving it.

If you have retrieved an existing role profile and you want to copy it to a new role profile, click the Copy button in the topmost row of buttons in the screen. The Copy Information screen is opened, and you can specify the Role ID and Description for the new role profile.

You can invoke ‘Role Definition’ screen by typing ‘SMDROLDF’ in the field at the top right corner of the Application tool bar and click the adjoining arrow. The screen is displayed below:



All the details of the existing profile are copied onto the new role profile. Again, you can change any of the details of the profile before saving it.

3.5.5 Deleting Role Profile

A Role Profile should be deleted only if there are no users linked to it. Thus, before deleting a role profile, you should modify each user profile attached to it and delete the link to the role.

To delete an existing role profile, retrieve the record of the role profile so that it is displayed in the main portion of the Role Definition screen. Then select the Delete button from the topmost row of buttons in the screen. If the role is linked to any user, a warning message will be displayed. This message will bring your attention to the fact that the user profile to which the role is linked will not be the same if the role profile is deleted.

You will be prompted to confirm the deletion. The Role Profile will be deleted only if you confirm the deletion.

3.5.6 Authorizing Role Profile

Before you link any users to a role, a user other than the one that defined it must authorize it. To authorize a role profile,

1. Retrieve the role profile record so that it is displayed in the Role Definition screen.
2. Click the Auth button from the topmost row of buttons in the screen. The Maintenance Authorization Details screen is displayed. The detail of each modification that was made to the record, in the sequence of occurrence is shown i n this screen. For each modification, the following details are displayed:

- The sequence number for the modification, in the Modification Number field.
- The record status of the modification, in the Record Status field.
- The user that effected the modification, in the Maker ID field.
- The date at which the modification occurred, in the Maker Date Stamp field.

- In Field Details in the lower grid portion, the changed values for each modification are displayed.

3. You can authorize any of the modified records, or all of them. Check the box in the Authorize? field in the desired row, to mark it for authorization.

When you have marked the required modifications for authorization, click the OK button to effect the authorization. The Maintenance Authorization Details screen is closed, and you are returned to the Role Definition screen.

3.5.7 Editing Role Profile

You can make changes to an authorized role profile as follows:

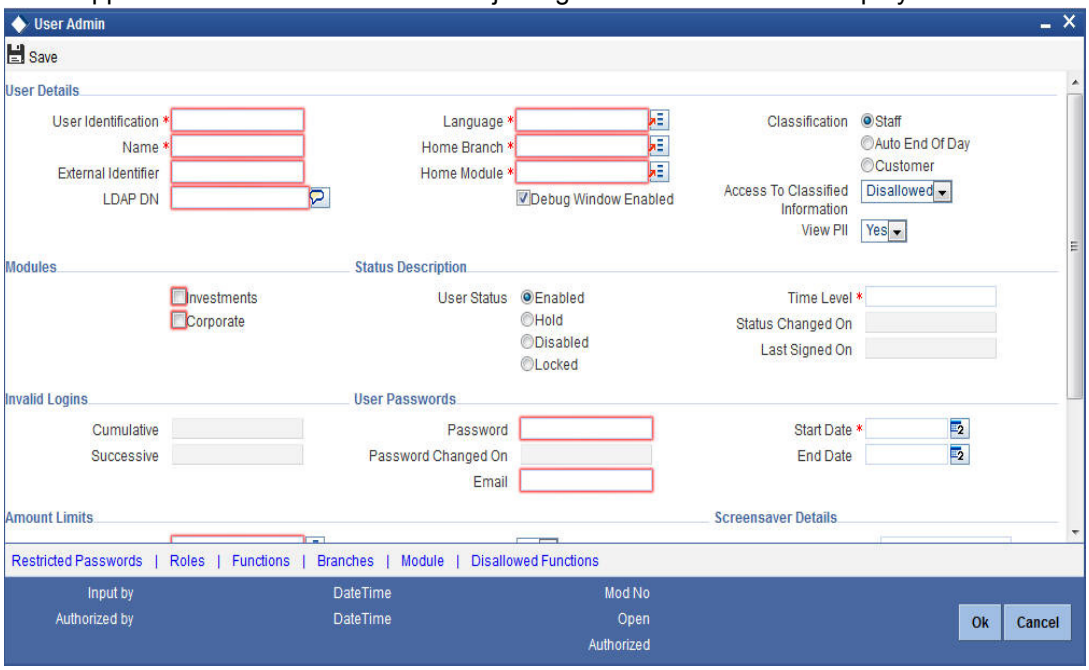
1. Retrieve the role profile record so that it is displayed in the Role Definition screen.
2. Click the Edit button from the topmost row of buttons in the screen. The record is now in readiness for modification.
3. After making your changes, click the Save button from the topmost row of buttons in the screen to save your changes. The record is now an edited, unauthorized record. Another user must now authorize it for it to be effective again.

3.6 Defining User Profile

A User Profile defines the activities that a user can carry out on the system. It also contains the user ID, the name through which the user will access the system and the password.

3.7 User Admin

You can invoke ‘User Admin’ screen by typing ‘SMDUSRDF’ in the field at the top right corner of the Application tool bar and click the adjoining arrow. The screen is displayed below:



Select 'New' from the Actions menu in the Application tool bar or click new icon to enter the details of the User Admin screen.

3.7.1 Fields in User Admin Screen

Specify the following basic information for the user profile, in the User Details section in this screen.

3.7.1.1 User Details Section

User Identification

Enter the unique identifier for the user, in the User Identification field. The minimum length of User Id must be six and the maximum number can be 12 characters.

External Identifier

Specify the External Identifier. External user is an alternative name for user id where two users can not have same External identifier.

Home Branch

The default branch that the user will login to the system from, in the Home Branch field

LDAP DN

The LDAP Details that have been maintained in the SSO screen have to be input here. Clicking on the 'Validate' button validates the LDAP details entered in the **Single Sign On.** The application will verify if only one user ID in FLEXCUBE Investor Service is mapped to the subject (DN) while authentication via SSO.

Name

The name of the user, in the Name field

Language

The default preferred language for the user, in the Language field

Classification

Select the classification of the user, that is, whether 'Staff', 'Customer' or 'Auto End of Day' from the options.

3.7.1.2 Modules Section

Select whether the user is a corporate modules user or an investment modules user.

Home Module

When you log into the system, you will be in the default module known as Home Module. Later you change the module according to your requirement.

3.7.1.3 User Status Module

Mandatory

The status of the user profile in the system is shown in this field. By default, every user profile is created as an enabled profile.

The status could be:

- Enabled – the profile is enabled and active in the system
- Hold – the status is on hold in the system.
- Disabled – it cannot be used to operate in the system

Status Changed On

Display Only

The most recent date on which the status of the user profile was changed is displayed here.

Time Level

Display Only

The most recent time at which the status of the user profile was changed is displayed here.

Last Signed On

Display Only

The most recent date on which the user logged in to the system is displayed here.

3.7.1.4 Password Section

Password

Alphanumeric, Mandatory

Specify the password using which the user will log in to the system. The static data AUTO_GEN_PASS_REQ is provided. The defaulted value 'Y' indicates whether the auto generation of the password is required or not.

> **Note**
>
> If the application level parameter which indicates the auto generation of the password is required or not is set to Y (Yes), then this field will be disabled and the system will create a random password in accordance with the parameters maintained at the level of the bank. The new password will be send to the respective user via mail.

At the time of setting up the Oracle FLEXCUBE Investor Servicing, the number of repeated successive parameters allowed in a password will be indicated.

For example, if the number of repeated successive parameters allowed in a password has been set as '2', then the user password can have a character repeating only twice. Suppose, if the number of repeated successive parameters has been specified as 2, a user password like AAA777 will be invalid. A valid password would be AA77.

Password Changed On

Display Only

The most recent date on which the password was changed is displayed here. When you are entering a new record, this field is blank and locked.

Email

Optional

Specify a valid Email id at the time of user creation. All system generated passwords shall be communicated to the user via this mail id.

Start Date

Date format, Optional

Specify the date on and following which the password is valid.

End Date

Date Format, Optional

Specify the date up to which the password is valid.

Note

The System is also configured to disallow the use of a pre-set number of previous passwords. This pre-set number is assigned at the time of installation, as a system parameter; the number can be subsequently changed if required, by changing this system parameter.

3.7.1.5 Amounts Limit Section

Transaction Amount

Numeric, Mandatory

Specify the maximum amount value that the user can specify while entering a transaction request from an investor.

Auth Amount

Numeric, Mandatory

Specify the maximum amount value of an investor transaction that the user can authorize.

Override Amount

Numeric, Mandatory

Specify the maximum amount value that the user can override while entering a transaction request from an investor.

Auto Auth

Select one of the following from the drop-down to indicate if auto authorisation is required or not:

- Yes
- No

Amount Format

Enter the amount format.

3.7.1.6 Invalid Logins Section

Successive

Numeric, Optional

Specify the number of successive invalid login attempts (in a single session) after which the user ID will be disabled for this profile.

Cumulative

Numeric, Optional

Specify the number of successive invalid login attempts (spread across different sessions) after which the user ID will be disabled for this profile.

After you have entered these basic details, you can specify any of the following information for the user profile, depending upon the necessity.

Note

When authentication of credentials is unsuccessful due to an incorrect user ID, then the user id will not be logged in the audit logs. In case the user id is correct and the password is wrong, the attempt is logged in the audit log and the successive and cumulative failure

count is incremented. When the user id and password are correct, this is logged into the audit logs.

3.7.2 Classifying User

You can classify a user as belonging to one of the following categories:

Staff	A user of the system who is an employee of your bank or AMC. You can include any of the functions available in the system in the user profile. Ideally, you should not include functions that are part of End of Cycle or End of Day operations in the profile of a Staff user.
Customer	A customer who would want to log into the system from a remote terminal. You can include only those functions through which the customer can inquire into balances and transactions.
AEOD	A user at the bank or AMC who is responsible for running the automated End of Day operations. You can include any of the functions available in the system in the user profile. Ideally, you should include only functions that are part of End of Cycle operations in the profile of an AEOD user.

You can indicate this through the Classification field in the User Profile Definition screen.

3.7.3 Interfacing with External Systems for Authentication

An external system can be used for level authentications. While logging into Oracle FLEXCUBE the authentication details are authenticated with the Oracle FLEXCUBE database and also with the external system database.

For instance, if the LDAP server is used level authentications, while logging into Oracle FLEXCUBE the authentication details are authenticated with the Oracle FLEXCUBE database and also with the LDAP database.

If LDAP is enabled for your installation, a user can log-in to FCIS using the 'Alternate User ID'. However, the maker and checked IDs will display the FCIS user ID only.

Note

Alternate User Id is mandatory if your installation is LDAP enabled.

3.7.4 Allowing User to Operate from Different Branches

When you create a User Profile, it will be attached to the branch where it is created. This means that the user can execute the functions defined for the profile from this branch. For a user profile, you can indicate that the user can access other branches also. The kind of functions a user can perform in a branch other than the one where the user profile is created depends on the category of the user.

3.7.4.1 Allowing User to Operate from Different Branches of AMC

For mutual fund account customers, you can define a list of branches of the AMC from which the user would be allowed to operate. To define this list, click the AMC button in the User Profile Definition screen.

3.7.4.2 User Belonging to Staff Category

In each branch, you should create a user profile called the Guest. The functions defined for this branch will be applicable for a user of a different branch. Typically, this profile should have access to functions like inquiry into balances, etc. If this Guest profile is not created in a branch, a user not belonging to that branch will not be allowed to change branch to it.

The branch where the user profile is created is called the Home branch and the other branches are called Host branches.

3.7.4.3 User Belonging to AEOD Category

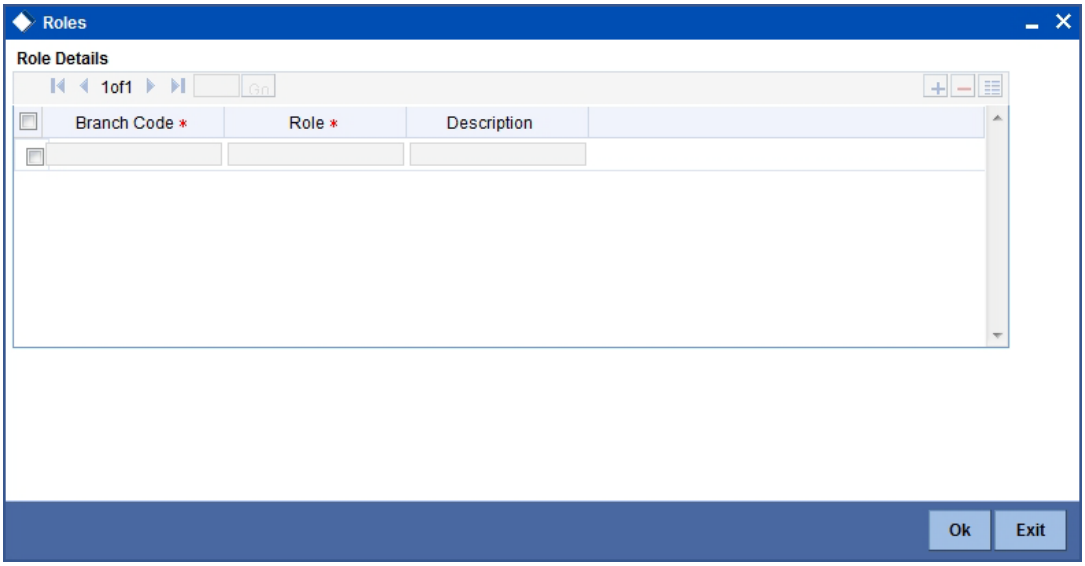
For such a user, the functions defined for the user profile where the profile created (the Home branch) will be applicable in every branch (Host branch).

3.7.4.4 User Belonging to Customer Category

A user of this category can log on only to the branch where the profile is created.

3.7.5 Roles for User

Click 'Roles' button in the bottom of the 'User Admin' screen to attach the user profile you are defining to a role. The User Roles screen will be displayed.



You can attach a role to the user profile, to be operable at a specific branch. Select a branch from the Branch Code field option list. Then click the Role ID field option list in the same branch row, to select the required rule profile. Click the option list icon for a list of role profiles that have been defined. To pick up a role from that list, double click on the role when it is highlighted.

To view the functions associated with the selected role, click the View button in the View Functions field. The User Role Functions view screen is displayed, with all the functions associated with the role.

A role profile could contain either back office (Fund Manager) functions or front office (Agency Branch) functions.

When you have selected the required roles, click the OK button to save your changes.

3.7.6 Functions for User

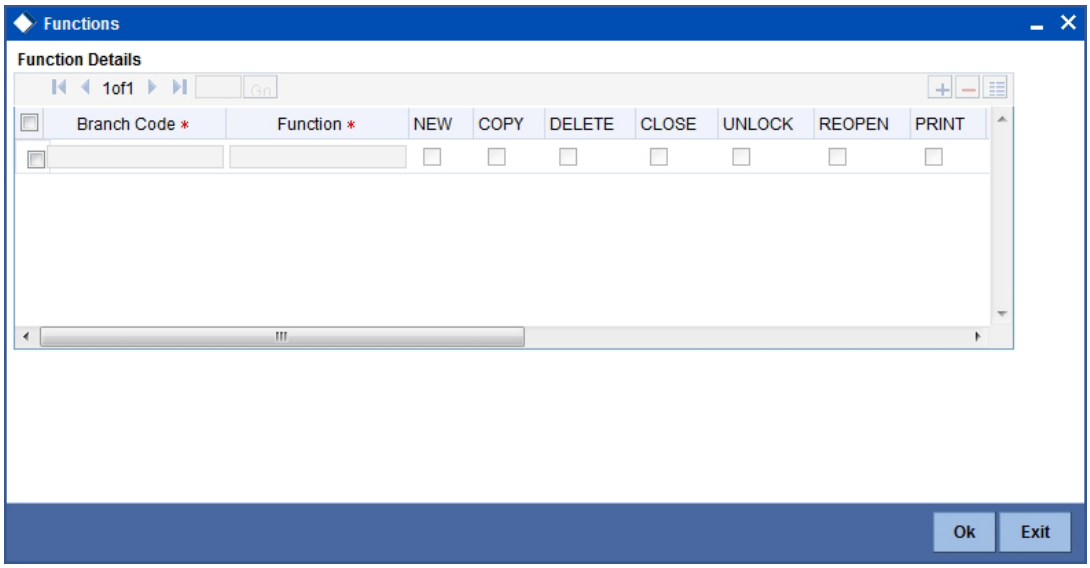
In addition to attaching a user profile to a role, you can give rights to individual functions. For a user profile to which no role is attached, you can give access to specific functions. If you have:

1. Attached one or more roles to a user profile, or
2. You have given access to individual functions to a profile to which roles are attached.

A user profile could be given access to either back office (Fund Manager) functions or front office (Agency Branch) functions, depending upon the tasks that the user has to perform within your organization.

The rights for Function IDs that figure in both the role and user specific functions will be applied as explained in the following example.

Click 'Functions' button in the bottom of the 'User Admin' screen to give access to functions for the user profile you are defining. The User Functions screen will be displayed.



The various functions in the system come under five categories. These categories and the icon in the User Functions screen that lets you define the rights for these categories are as follows:

Category	Description	Button Name
Maintenance	Functions relating to the setting up of investor accounts and brokers.	Mainte-nance
Transactions Input	Functions relating to the entry of investor transactions.	
Batch	Functions relating to the automated operations like End of Day Processes.	Batch
Reports	Functions relating to the generation of reports in the various modules.	Reports
On-line	Functions relating to contract processing.	On-line

When the functions in a selected menu are listed, select the row representing the function that you want to link to the user profile.

For each function, you can allow or disallow specific record-level operations. These operations are displayed as a horizontal list, alongside the Maintenance Functions label, with each operation spelled out vertically.

In the selected function row, check the box pertaining to each operation you want to allow for the user profile.

You can allow any of the following operations at record level for the user profile, in any function:

3.7.6.1 Static Screens

- NEW (Define a new record).
- COPY (Copy details of an existing record).
- DELETE (Delete an existing record).
- CLOSE (Close an existing record).
- UNLOCK (to amend an existing record).
- REOPEN (Reopen an existing record).
- PRINT (Print the details of selected records).
- AUTH (Authorize any maintenance activity on a record).
- REVERSE
- ROLLOVER
- CONFIRM
- LIQUIDATE
- HOLD
- TEMPLATE
- VIEW
- GENERATE

3.7.6.2 Contracts and On-Line Transaction Processing

- VIEW (to see the details of the contract).

3.7.6.3 Reports

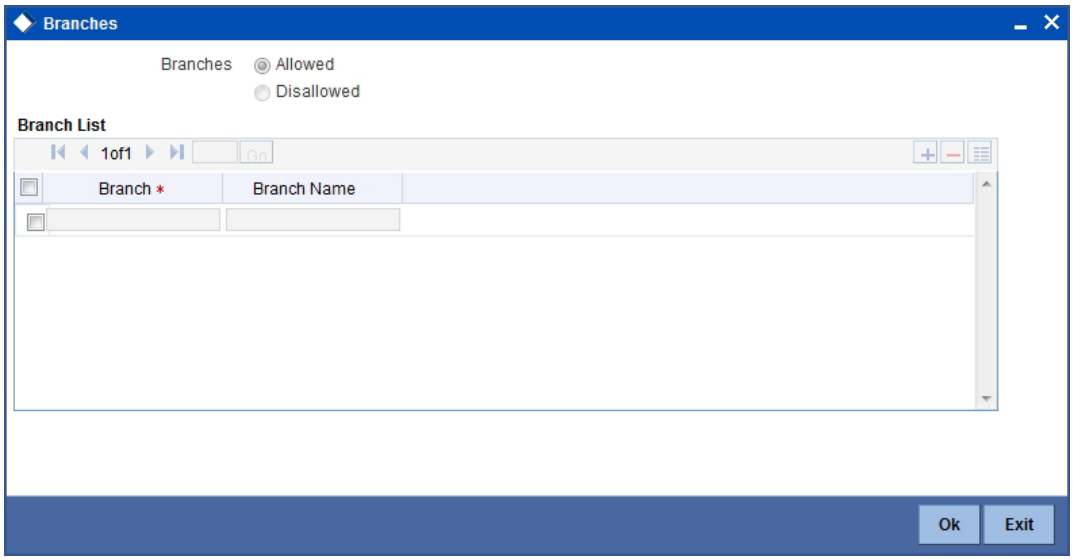
- GENERATE (to generate reports).
- VIEW (view the reports).
- PRINT (print the reports).

To delete the access rights you have specified for a function, select the required Function ID row and check the Delete box to the left of the Function ID field.

To edit the access rights you have specified for a function, select the required Function ID row and check the Edit box to the left of the Delete field.

3.7.7 Branches for User

For Staff and End of Day users, you can specify the branches from which they can operate. Click ‘Branches’ button in the bottom of the ‘User Admin’ screen to define the branches in which the user should be allowed to operate.



To prepare a list of branches from which the user is disallowed, choose the Disallowed option.

Then, using the arrows, move any required branch found in the Available box to the Disallowed box, and click ‘Ok’ button.

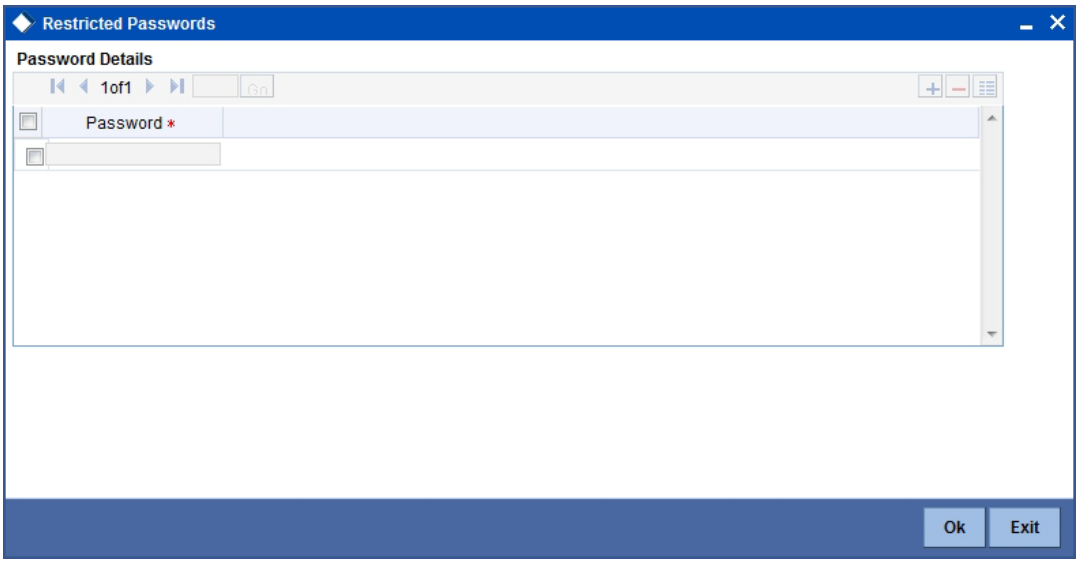
Similarly, to prepare a list of branches from which the user is allowed to operate, choose the Allowed option.

Then, using the arrows, move any required branch found in the Available box to the Allowed box, and click ‘Ok’ button.

3.7.8 Restrictive Passwords for User

You can maintain a list of passwords that the user is most likely to use. For example, a user may tend to use the names of loved ones, the AMC or AMC branch, department, etc. as a password as they are easy to remember. This might be a security risk as it will be easy for another person to guess a password. To prevent this, you can maintain a list of passwords that the user should not use. This list of restrictive passwords will be checked before a password is accepted when the user is changing passwords. If the password entered by the user is listed, it will not be accepted.

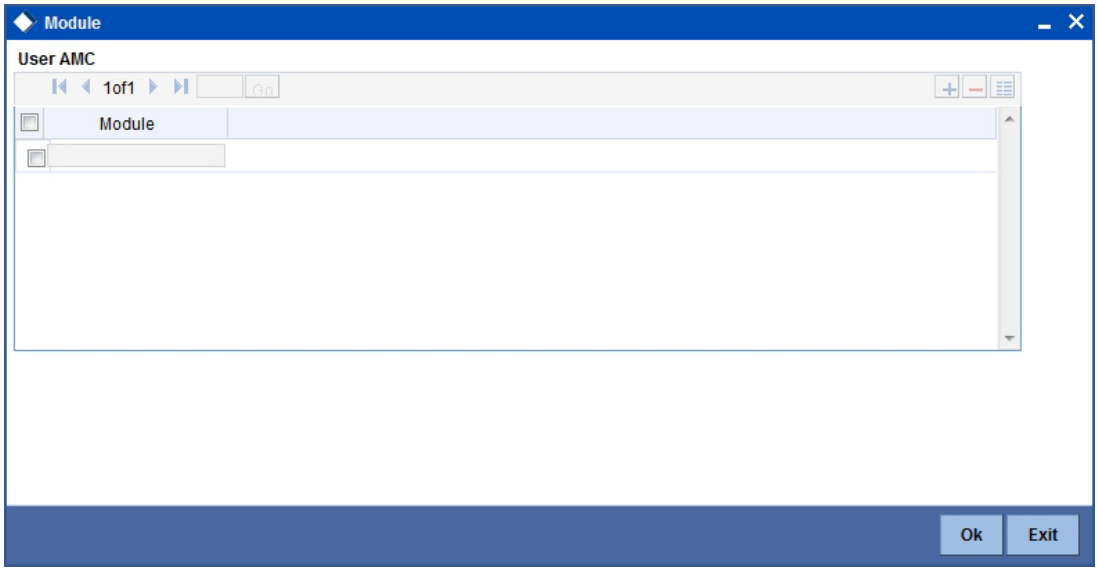
Click ‘Restricted Passwords’ button in the bottom of the ‘User Admin’ screen, left margin of the screen. The Restrictive Passwords screen is opened, where you can define a list of such passwords.



The user for whom you are defining the restrictive passwords cannot use restrictive passwords defined in the Role Profile screen.

3.7.9 AMCs for User

You can restrict the user to operate only from certain AMCs, or certain branches of an AMC. To define such a restrictive list of AMCs or AMC branches, click ‘Module’ button in the ‘User Admin’ screen.The User AMC screen is opened.

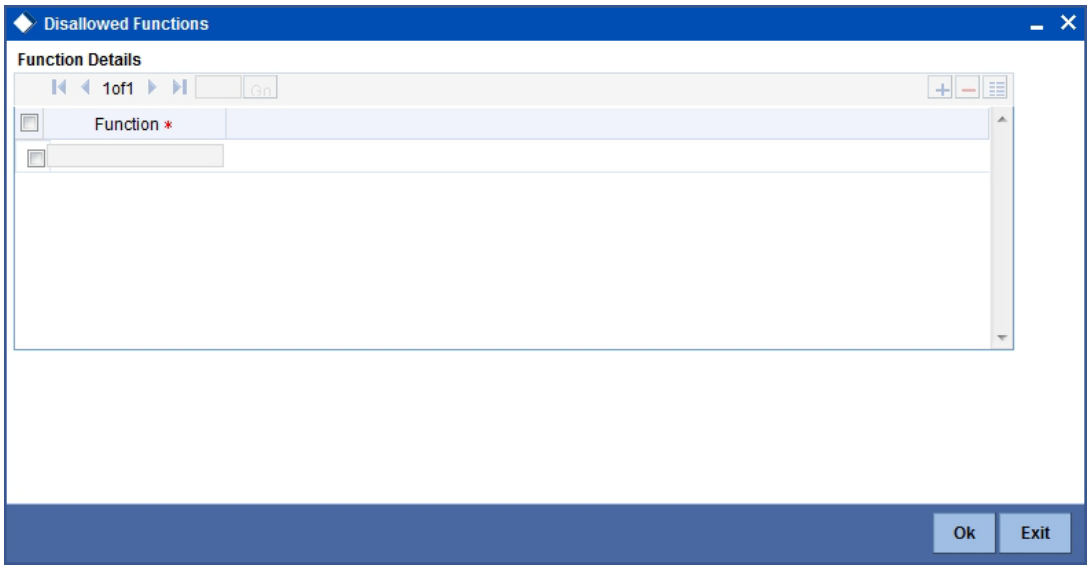


To allow the user to operate the system from a certain AMC, select it in the Available box, and move it to the Allowed box using the arrows. When you have selected the required AMCs, click the OK button to save your changes.

3.7.10 Disallowed Functions for Users

You can define a list of functions that the user is not allowed to operate, out of the functions list already associated with the user profile. To define such a restrictive list of functions, click ‘Disallowed Functions’ button in the bottom of the ‘User Admin’ screen.

The User Function Disallowed screen is opened. All the functions that are associated with the user profile are listed in the Available box.



To disallow a function, select it in the Available box and move it to the Disallowed box using the arrows. After selecting and moving all required functions in such a manner, click OK to save your changes.

3.7.11 Other Attributes for User Profile

Other than the attributes you have defined for a user profile, such as the role association, function access rights, restrictive passwords and branch restrictions, you can define any of the following attributes. Click on the appropriate button in the group of buttons displayed in the left margin of the screen:

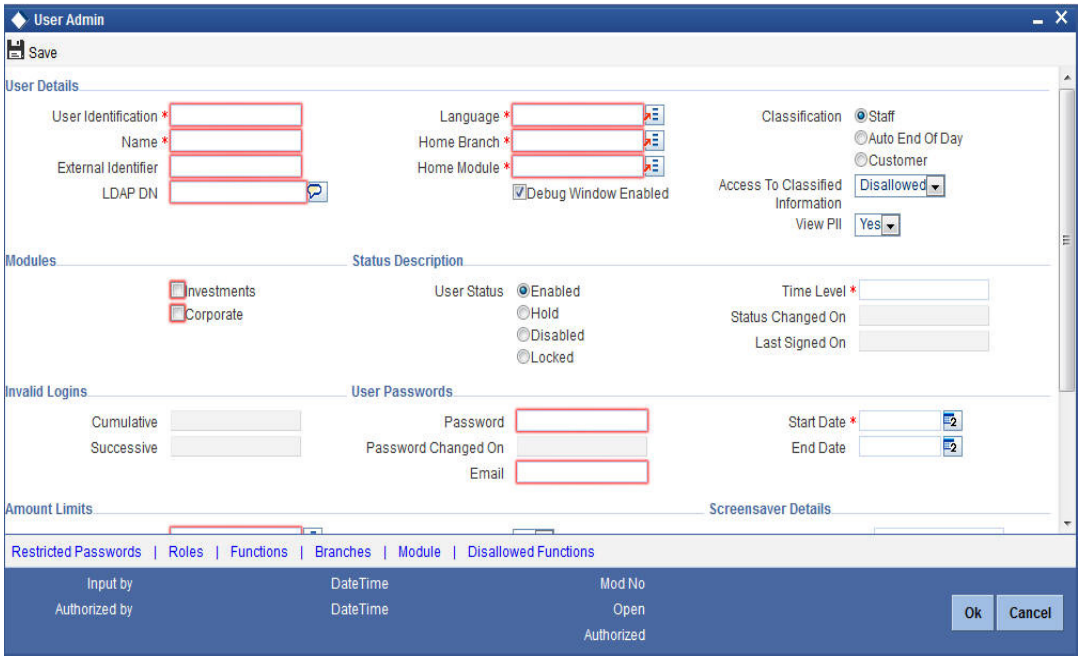
- The Rights button to define grant rights and grant queues for the user profile
- The User Till Restrictions button to define till restrictions for the user profile.
- The User Account Class Restrictions button to define a restrictive list of account classes for the user profile.
- The User GL Restrictions button to define a restrictive list of Node GL's and sub nodes.

3.7.12 Copying User Profile of Existing User

Often, you may have to create a user profile that closely resembles an existing one. In such a case, you can copy the existing profile on to the new one.

Choose the Copy button from the row of buttons at the topmost row of the screen. A list of existing user profiles will be displayed. Click on the one you want to copy. All the details of the profile except the User ID will be copied and displayed. Enter a unique User ID. You can change any of the details of the profile before saving it.

If you have retrieved an existing user profile and you want to copy it to a new user profile, click the Copy button in the topmost row of buttons in the screen. The Copy Information screen is opened, and you can specify the User ID for the new user profile.



All the details of the existing profile are copied onto the new user profile. Again, you can change any of the details of the profile before saving it.

3.7.13 Deleting User Profile

A user profile can be deleted only if the user is currently not logged on to the system.

To delete an existing user profile, retrieve the record of the user profile so that it is displayed in the main portion of the User Profile Definition screen. Then select the Delete button from the topmost row of buttons in the screen. If the user is logged in to the system, a warning message will be displayed and you cannot delete the profile.

If the user is not logged in, you will be prompted to confirm the deletion. The user profile will be deleted only if you confirm the deletion.

3.7.14 Authorizing User Profile

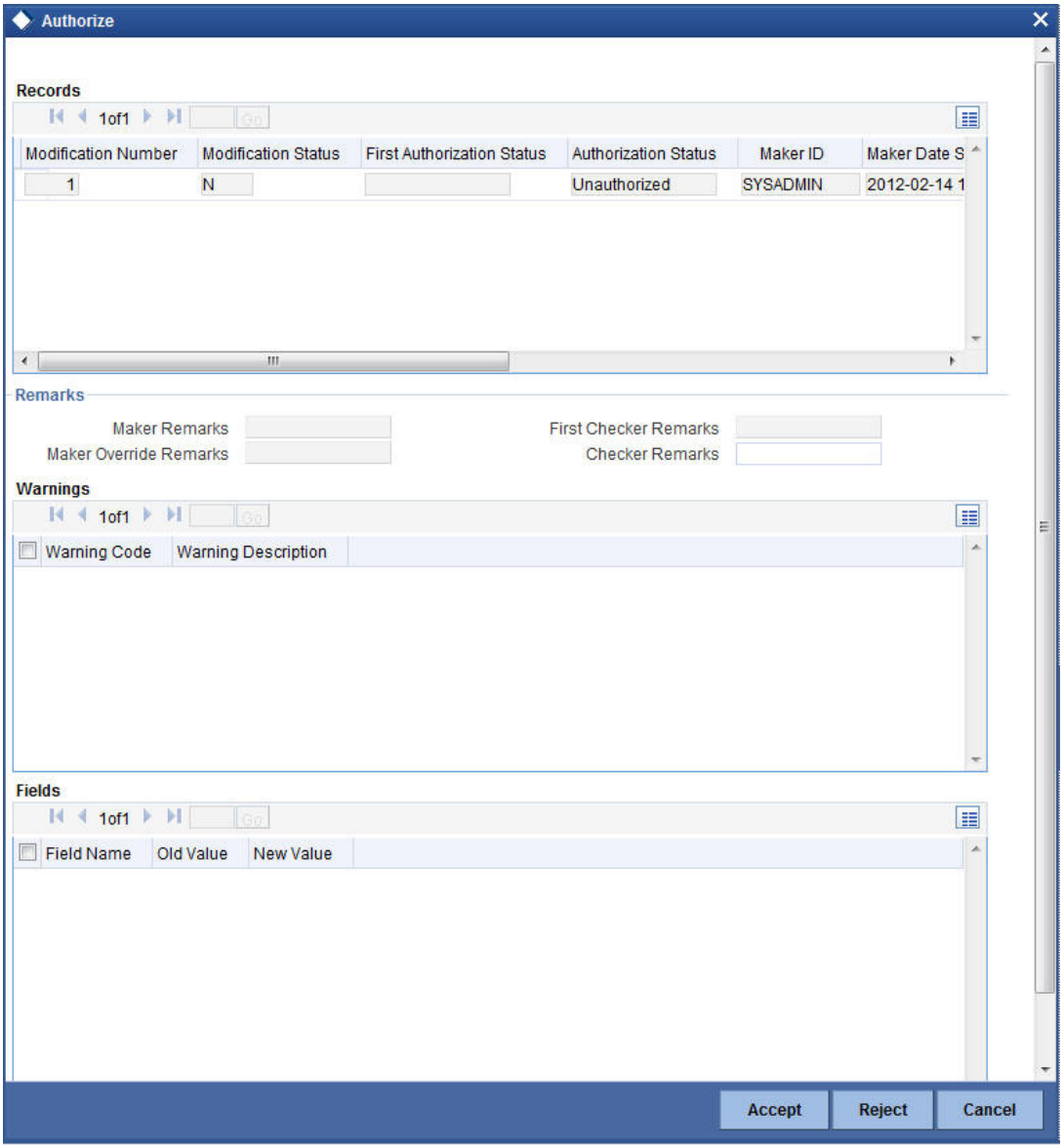
Before you link any users to a user, a user other than the one that defined it must authorize it.

To authorize a user profile,

1. Retrieve the user profile record so that it is displayed in the User Definition screen.
2. Click the Auth button from the topmost row of buttons in the screen. The Maintenance Authorization Details screen is displayed. The details of each modification that was made to the record, in the sequence of occurrence is shown in this screen. For each modification, the following details are displayed:
   - The sequence number for the modification, in the Mod No. field.
   - The status of the modification, the Record Status.
   - The user that effected the modification, in the Maker ID.
   - The date at which the modification occurred, in the Maker Date Stamp.
   - In the Field Details, the changed values for each modification are displayed.

3. You can authorize any of the modified records, or all of them. Check the box in the Authorize? field in the desired row, to mark it for authorization.

When you have marked the required modifications for authorization, click the OK button to effect the authorization. The Maintenance Authorization Details screen is closed, and you are returned to the User Definition screen.



3.7.15 Editing User Profile

You can make changes to an authorized user profile as follows:

1. Retrieve the user profile record so that it is displayed in the User Profile Definition screen.
2. Click the Edit button from the topmost row of buttons in the screen. The record is now in readiness for modification.
3. After making your changes, click the Save button from the topmost row of buttons in the screen to save your changes. The record is now an edited, unauthorized record. Another user must now authorize it for it to be effective again.

Status Bar Information

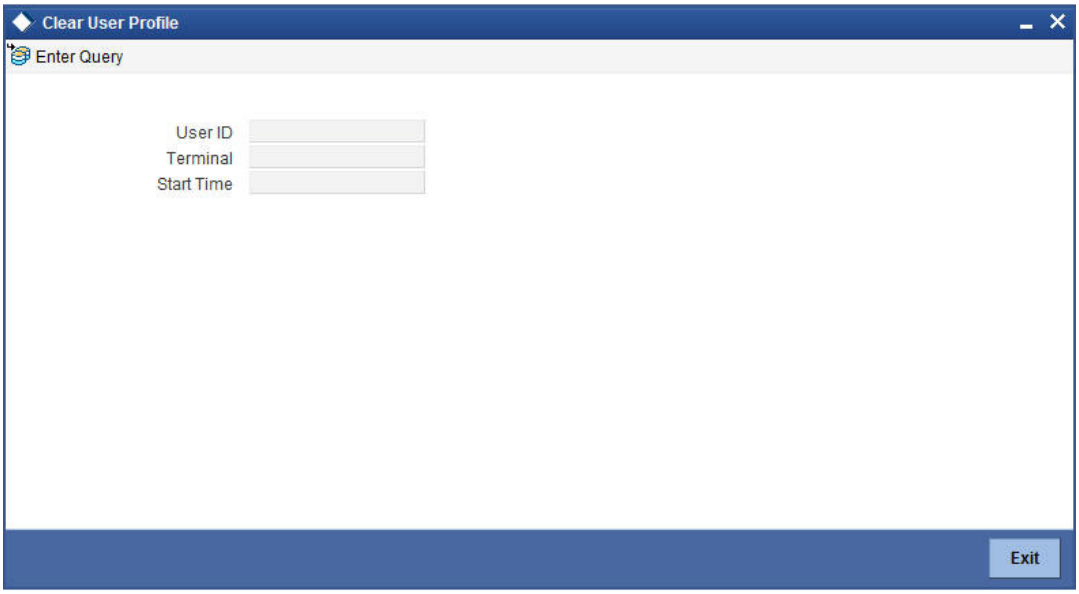
In this section, the following details are displayed for any user profile record:

- The user that has created the user profile, in the Input By field.
- The date and time of user profile creation, in the Date Time field.
- The user that has authorized the user profile, in the Authorized By field.
- The date and time of user profile authorization, in the Date Time field.
- The serial sequence number of the most recent modification of the user profile, in the Mod No field.
- The authorization status of the record, in the Authorize field.
- The open status of the record, in the Open field.

3.8 Clearing User That Has Exited

If a user exits the system abnormally, the administrative users can clear the logged in user profile so that the user can log in normally again. To clear a logged-in user in this manner, the Control Clerks need not login also.

To clear a user, log in to the system as an administrative user, and typing 'SMDCLUSR' in the field at the top right corner of the Application tool bar and click the adjoining arrow. The Clear Users screen is displayed.



To clear a user, you need to unlock and save after entering the above mentioned details.

3.9 Enabling Auto Authorization

Most of the information that you enter in to the system needs to be authorized to be effective. Except for the static information that you typically enter in to the system only once, all other information must be authorized. Authorization is required for all maintenance as well as transactional information in the system

When you enter information related to any of these events into the system, the record that is initially saved when you complete the data entry is retained in the system as unauthorized information, which must be subsequently authorized to become effective.

Usually, authorizing information in the system is an activity that follows a maker-checker concept, i.e., the user that enters the information must be necessarily different from the user that authorizes the information. Therefore, whereas one user group will have access to functions that involve entering information into the system, a different user group has access to the functions that involve information authorization, and there is no overlap of access privileges.

3.10 Auto-authorization Features in System

In some environments, the user that enters the information needs to be able to authorize it simultaneously. In such cases, the maker-checker concept leads to unnecessary delegation of activity, which is undesirable. This means that in such an environment, the user that enters the information must, on saving the entered record, be able to authorize the record. For such environments, the auto-authorization function is provided by the FC-IS system. When this function is used, the Save operation in any screen that involves data entry (apart from static information screens) will also invoke and perform the authorization for the records that have been entered.

It is possible to be selective about the business functions for which you need to use the auto-authorization feature. This means that you can enable the auto-authorization feature for the functions for which you require simultaneous authorization on saving the record, and you can keep it disabled for others, allowing them to go through the normal maker-checker process of authorization.

The following features comprise the auto-authorization facility in the system:

- The user administrator users can map the business users to the menu items, and make auto-authorization feature allowable for any business user – menu item mapping. All business checks, validations and processes that must be performed when the authorization happens will be triggered immediately following the use of the save operation, when the auto-authorization feature is allowed.
- The user administrator users can enable (or disable) auto authorization rights at a user group level. Any user roles and / or users associated with the user group would inherit the auto authorization privileges assigned to the user group. If a user ID is associated with multiple user roles, the most restrictive privilege assigned to the roles will be applicable.
- You can enable (or disable) the auto authorization feature for data operations in the New mode or the Amend mode, including data entry either for reference information, investor accounts or transactions. For transaction entry operations in either mode, you can enable (or disable) auto authorization for transactions involving any of the following circumstances:
  - Transactions for which the transaction currency is the limit currency, and the transaction amount falls within the limit amount for that currency
  - Back dated transactions
  - Transactions in respect of which applicable loads have been overridden
  - Transactions for which third party payment or delivery has been specified

3.10.1 Using Auto-authorization Feature

To allow the auto-authorization feature for a user group and a certain set of menu items, you must map the user groups to the menu items or the task for which auto-authorization is applicable, using the ‘Auto Auth Maintenance’ screen. You can access this screen by clicking Security Maintenance menu and selecting Auto Auth from the Browser.

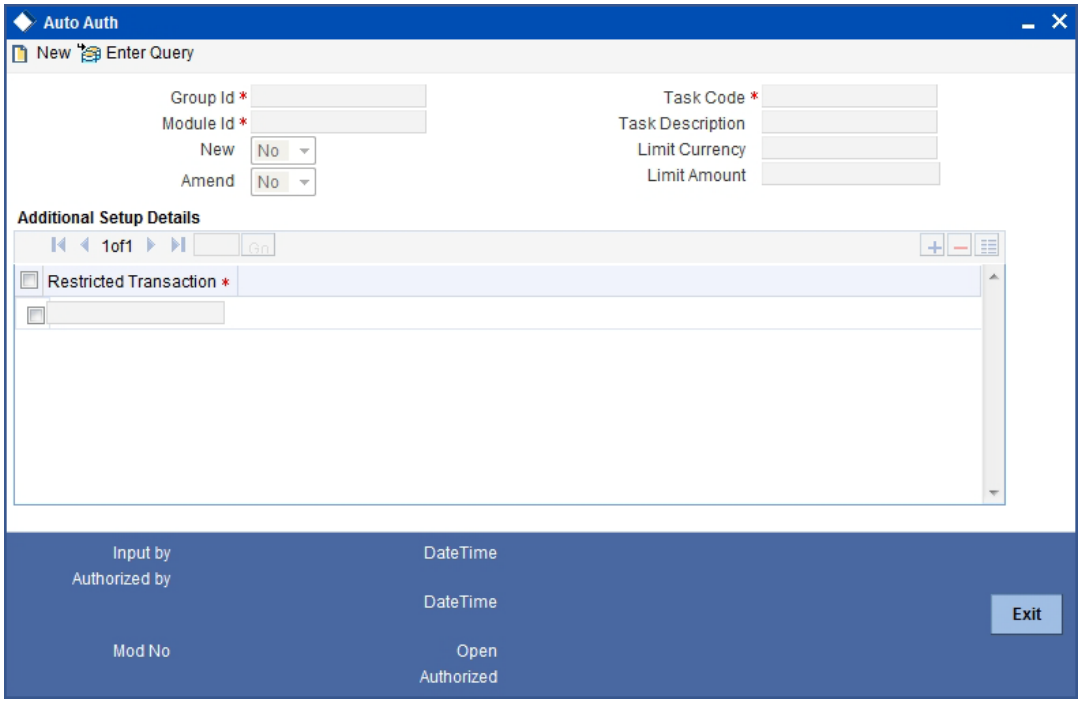
3.10.2 Auto Auth Maintenance Screen

You can use this screen to map user groups to the tasks for which auto-authorization is applicable. If the user administrator or the module administrator users do not maintain the setup for each of the user groups in this screen, the auto-authorization is not enabled for that user group.

3.10.3 Enabling Or Disabling Auto-Authorization User Group

When you open the Auto Auth Maintenance screen, the auto authorization features that have been enabled for the module and the group to which the logged in user belongs, are displayed.

You can invoke this screen by typing 'SMDAUTAU' in the field at the top right corner of the Application tool bar and click the adjoining arrow. The screen is displayed below:



3.10.4 Fields in Auto Auth Screen

Group ID

Mandatory

Select the Group ID from the option list.

Module ID

Mandatory

Select the Module ID from the option list.

Task Code

Mandatory

Select the Task Code from the option list.

New

Optional

You can select 'Yes' to indicate new.

Amend

Optional

You can select 'Yes' to amend.

Limit Currency

Optional

Select the limit currency from the option list.

Limit Amount

Optional

Enter the limit amount.

3.10.4.1 Additional Setup Details Section

Restricted Transaction

To amend the displayed list, select 'Unlock' from the Actions menu in the Application toolbar or click unlock icon. The screen is displayed in Amend mode, where you can make your changes. The changes you make will apply to all users and roles in the Group ID to which the logged in user belongs, for the logged in Module.

You can make changes as follows:

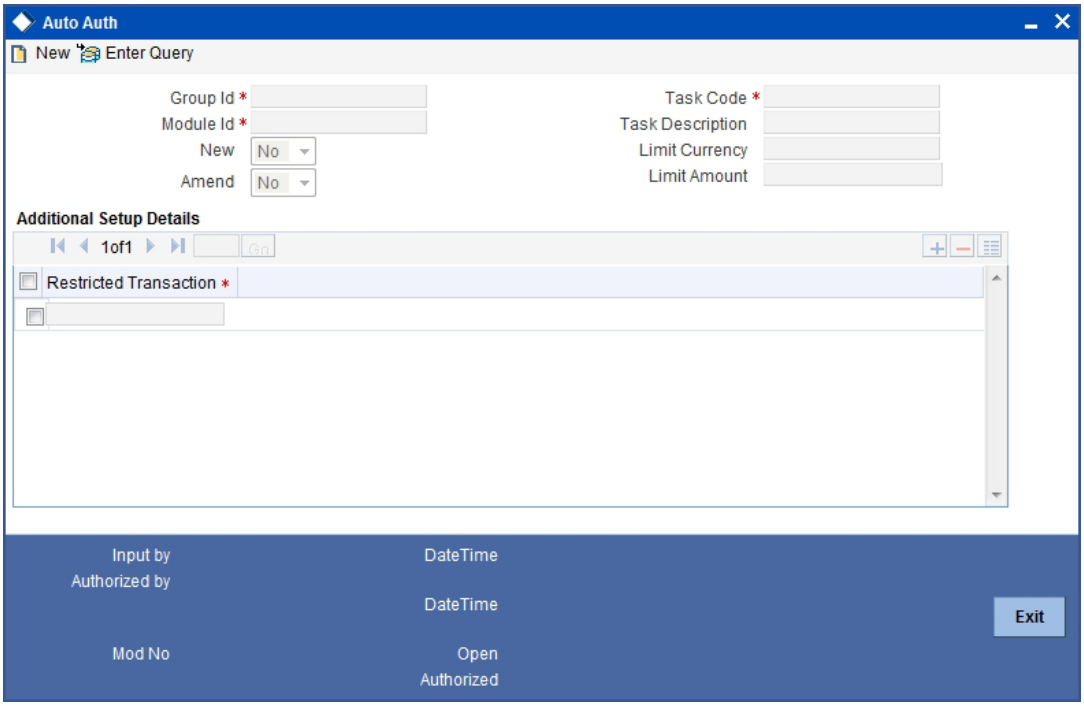
- To enable auto-authorization in the New mode for a task item, select 'YES' in the Newfield for the task item. To enable auto-authorization in the Amend mode for a task, select 'YES' in the Amend field for the task item.
- For transaction data entry task items, you can limit the volume of the transactions that can be auto-authorized. To setup this limit, specify the highest volume of the transaction that can be auto-authorized, in the Limit Amount field. You must also indicate the currency in which the volume you have specified is reckoned, in the Limit Currency field. You can indicate a different limit for each role or Group ID, if necessary.
- For transaction data entry, you can also enable (or disable) the auto authorization feature for transactions in the following circumstances:
- Back dated transactions. Select 'YES' in the Restrict Back Dated Transaction field to disable auto authorization of backdated transactions in the selected mode. Select 'NO' to enable auto authorization of backdated transactions in the selected mode.
- Transactions in respect of which applicable loads have been overridden. Select 'YES' in the Restrict Load Override Transactions field to disable auto authorization of load override transactions in the selected mode. Select 'NO' to enable auto authorization of load override transactions in the selected mode.
- Transactions for which third party payment has been specified. Select 'YES' in the Restrict Third Party Payment Transactions field to disable auto authorization of third party payment transactions in the selected mode. Select 'NO' to enable auto authorization of third party payment transactions in the selected mode.
- Transactions for which third party delivery has been specified. Select 'YES' in the Restrict Third Party Delivery Transactions field to disable auto authorization of third party delivery transactions in the selected mode. Select 'NO' to enable auto authorization of third party delivery transactions in the selected mode.
- When you have finished making the auto-authorization specification for a user group, click save icon .

When you have finished making your auto-authorization specifications for each user group in this screen, and saved your changes, the auto-authorization feature is enabled, and when the user invokes the Save operation in any of the applicable task screens, the entered records are saved as authorized records.

To enable auto authorization for a user group other than the logged in user group, click save icon in the Auto Auth Maintenance screen.

The system displays the message as “Are you sure you want to close the current record?”.

Click ‘Ok’ button. The auto authorization record of the logged in user group, which was on display, is closed, and the Auto Auth Maintenance screen is opened in New mode.



Select the user group for which you want to enable or disable the auto authorization rights, in the Group ID field. Select the corresponding module in the Module ID field, and click OK.

Subsequently, proceed to set up the auto authorization rights in the same manner as described above, for the amend operation.

3.10.4.2 How Auto Authorization Privileges Are Applied

The examples given below explain how auto authorization privileges could be granted, and how they are applied in the system:

3.10.5 Operations on Auto Authorization Records

After you have set up auto authorization for a user group, you must have another user authorize it so that it would be effective in the system.

Before the setup is authorized, you can edit its details as many times as necessary. You can also delete it before it is authorized.

After authorization, you can only make changes to any of the details through an amendment.

The Auto Auth Maintenance screen can be used for the following operations on auto authorization setups:

- Retrieval for viewing
- Editing unauthorized setups
- Deleting unauthorized setups
- Authorizing setups
- Amending authorized setups.

To perform these operations, click on the appropriate buttons in the horizontal array of buttons in the Auto Auth Maintenance screen.

4. Enabling Auto Authorization

4.1 Normal Process of Authorization in System

Most of the information that you enter in to

the system needs to be authorized to be effective. Except for the static information that you typically enter in to the system only once, all other information must be authorized. Authorization is required for all maintenance as well as transactional information in the system.

When you enter information related to any of these events into the system, the record that is initially saved when you complete the data entry is retained in the system as unauthorized information, which must be subsequently authorized to become effective.

Usually, authorizing information in the system is an activity that follows a maker-checker concept, i.e., the user that enters the information must be necessarily different from the user that authorizes the information. Therefore, whereas one user group will have access to functions that involve entering information into the system, a different user group has access to the functions that involve information authorization, and there is no overlap of access privileges.

4.2 Auto-authorization Features in System

In some environments, the user that enters the information needs to be able to authorize it simultaneously. In such cases, the maker-checker concept leads to unnecessary delegation of activity, which is undesirable. This means that in such an environment, the user that enters the information must, on saving the entered record, be able to authorize the record. For such environments, the auto-authorization function is provided by the FC-IS system. When this function is used, the Save operation in any screen that involves data entry (apart from static information screens) will also invoke and perform the authorization for the records that have been entered.

It is possible to be selective about the business functions for which you need to use the auto-authorization feature. This means that you can enable the auto-authorization feature for the functions for which you require simultaneous authorization on saving the record, and you can keep it disabled for others, allowing them to go through the normal maker-checker process of authorization.

The following features comprise the auto-authorization facility in the system:

- The user administrator users can map the business users to the menu items, and make auto-authorization feature allowable for any business user – menu item mapping. All business checks, validations and processes that must be performed when the authorization happens will be triggered immediately following the use of the save operation, when the auto-authorization feature is allowed.
- The user administrator users can enable (or disable) auto authorization rights at a user group level. Any user roles and / or users associated with the user group would inherit the auto authorization privileges assigned to the user group. If a user ID is associated with multiple user roles, the most restrictive privilege assigned to the roles will be applicable.
- You can enable (or disable) the auto authorization feature for data operations in the New mode or the Amend mode, including data entry either for reference information, investor accounts or transactions. For transaction entry operations in either mode, you can

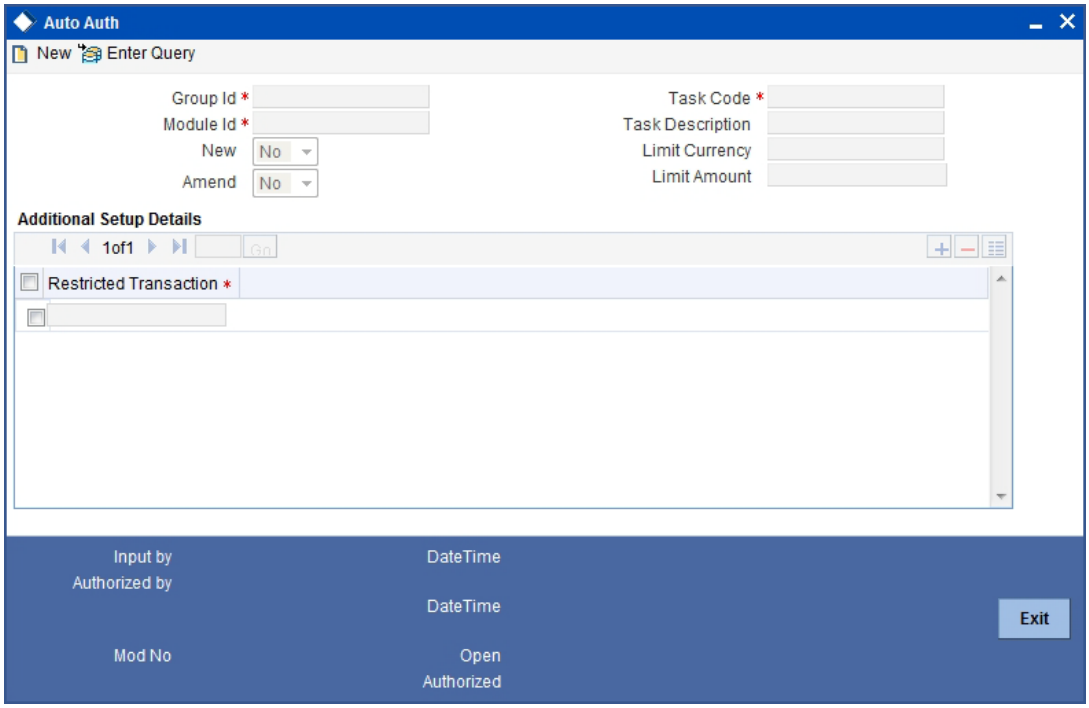
enable (or disable) auto authorization for transactions involving any of the following circumstances:

- Transactions for which the transaction currency is the limit currency, and the transaction amount falls within the limit amount for that currency
- Back dated transactions
- Transactions in respect of which applicable loads have been overridden
- Transactions for which third party payment or delivery has been specified

4.2.1 Using Auto-authorization Feature

To allow the auto-authorization feature for a user group and a certain set of menu items, you must map the user groups to the menu items or the task for which auto-authorization is applicable, using the 'Auto Auth Maintenance' screen.

You can invoke this screen by typing 'SMDAUTAU' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button. The screen is displayed below:

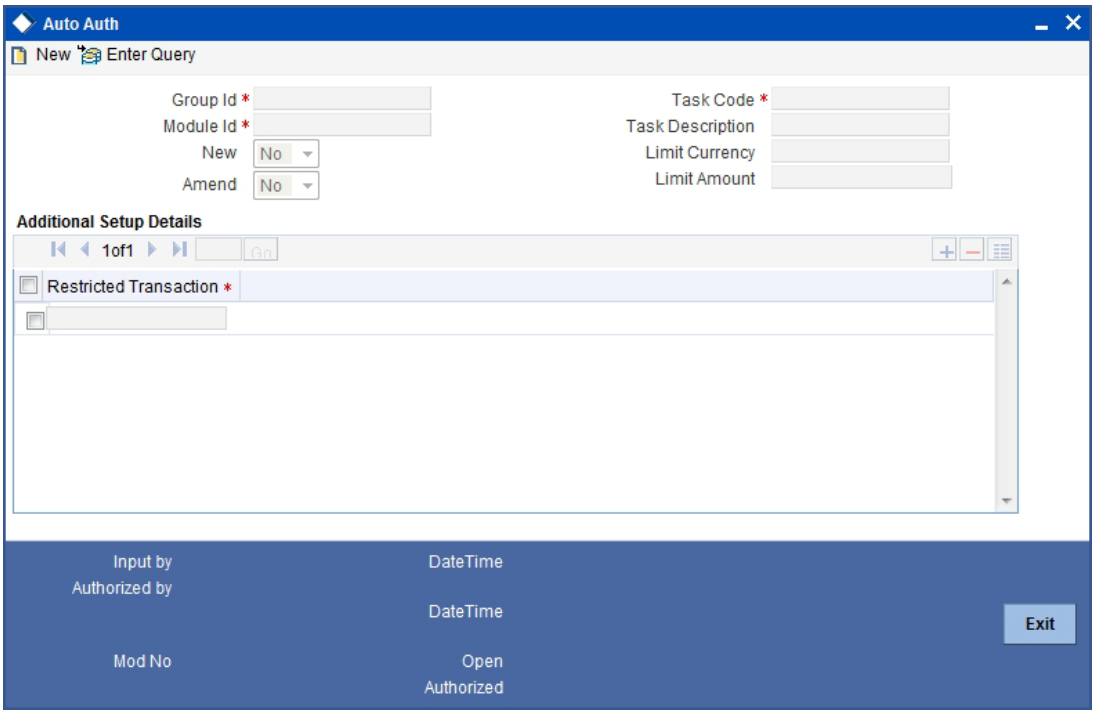


4.2.1.1 Auto Auth Maintenance Screen

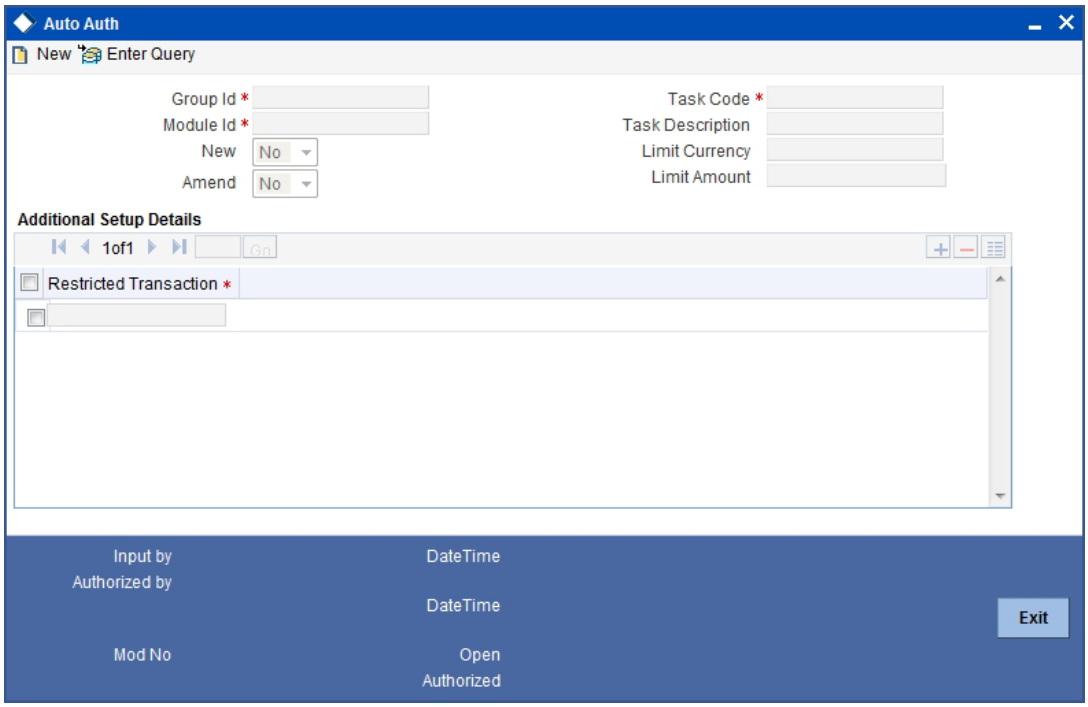
You can use this screen to map user groups to the tasks for which auto-authorization is applicable. If the user administrator or the module administrator users do not maintain the setup for each of the user groups in this screen, the auto-authorization is not enabled for that user group.

4.2.1.2 Enabling or Disabling Auto-authorization for User Group

When you open the Auto Auth Maintenance screen, the auto authorization features that have been enabled for the module and the group to which the logged in user belongs, are displayed.



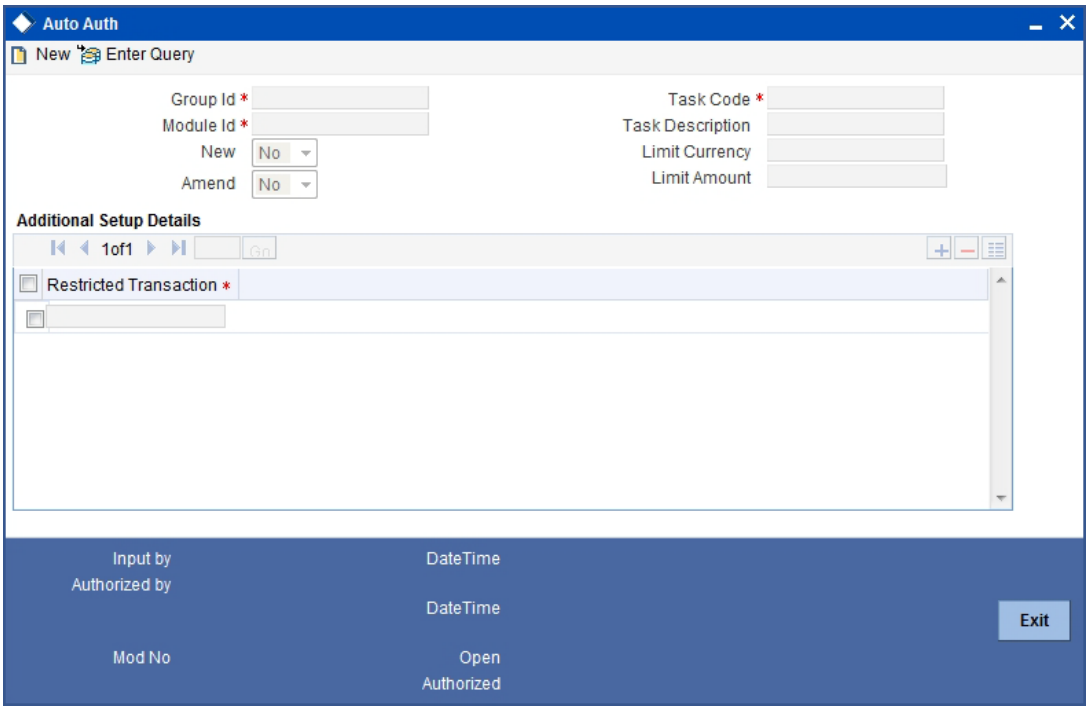
To amend the displayed list, click unlock icon. The screen is displayed in Amend mode, where you can make your changes. The changes you make will apply to all users and roles in the Group ID to which the logged in user belongs, for the logged in Module.



You can make changes as follows:

- To enable auto-authorization in the New mode for a task item, select ‘YES’ in the Newfield for the task item. To enable auto-authorization in the Amend mode for a task, select ‘YES’ in the Amend field for the task item.
- For transaction data entry task items, you can limit the volume of the transactions that can be auto-authorized. To setup this limit, specify the highest volume of the transaction that can be auto-authorized, in the Limit Amount field. You must also indicate the currency in which the volume you have specified is reckoned, in the Limit Currency field. You can indicate a different limit for each role or Group ID, if necessary.
- For transaction data entry, you can also enable (or disable) the auto authorization feature for transactions in the following circumstances:
- Back dated transactions. Select ‘YES’ in the Restrict Back Dated Transaction field to disable auto authorization of backdated transactions in the selected mode. Select ‘NO’ to enable auto authorization of backdated transactions in the selected mode.
- Transactions in respect of which applicable loads have been overridden. Select ‘YES’ in the Restrict Load Override Transactions field to disable auto authorization of load override transactions in the selected mode. Select ‘NO’ to enable auto authorization of load override transactions in the selected mode.
- Transactions for which third party payment has been specified. Select ‘YES’ in the Restrict Third Party Payment Transactions field to disable auto authorization of third party payment transactions in the selected mode. Select ‘NO’ to enable auto authorization of third party payment transactions in the selected mode.
- Transactions for which third party delivery has been specified. Select ‘YES’ in the Restrict Third Party Delivery Transactions field to disable auto authorization of third party delivery transactions in the selected mode. Select ‘NO’ to enable auto authorization of third party delivery transactions in the selected mode.
- When you have finished making the auto-authorization specification for a user group, click save icon to save your changes.
- When you have finished making your auto-authorization specifications for each user group in this screen, and saved your changes, the auto-authorization feature is enabled, and when the user invokes the Save operation in any of the applicable task screens, the entered records are saved as authorized records.
- To enable auto authorization for a user group other than the logged in user group, click save icon in the Auto Auth Maintenance screen. The system displays the message as “Do you want to cancel the operation?”

Click on the ‘OK’ button. The auto authorization record of the logged in user group, which was on display, is closed, and the Auto Auth Maintenance screen is opened in New mode.



Select the user group for which you want to enable or disable the auto authorization rights, in the Group ID field. Select the corresponding module in the Module ID field, and click on ‘Ok’ button.

Subsequently, proceed to set up the auto authorization rights in the same manner as described above, for the amend operation.

4.2.2 Operations on Auto Authorization Records

After you have set up auto authorization for a user group, you must have another user authorize it so that it would be effective in the system.

Before the setup is authorized, you can edit its details as many times as necessary. You can also delete it before it is authorized.

After authorization, you can only make changes to any of the details through an amendment.

The Auto Auth Maintenance screen can be used for the following operations on auto authorization setups:

- Retrieval for viewing
- Editing unauthorized setups
- Deleting unauthorized setups
- Authorizing setups
- Amending authorized setups.

To perform these operations, click on the appropriate buttons in the horizontal array of buttons in the Auto Auth Maintenance screen.

4.3 PIPA Audit Log

This section contains the following topic:

- Section 4.3.1, "Uploading PIPA Audit Log"

4.3.1 Uploading PIPA Audit Log

As per Article 12 of Enforcement Rules of Personal Information Protection Act which is enacted according to Article 55 of the Personal Information Protection Act ('the Act'), the government agency or the non-government agency will have to take technical or organizational measures for the purpose of preventing personal information from being stolen, altered, damaged, destroyed or disclosed. This includes but is not limited to establishing a mechanism of auditing information security and keeping records of the use, locus information and proof.

You can log audit information to access unit holder/ customer/ transaction and balance related information. The system will store the details of data accessed by the business user for the current day. The data access log covers the following data:

- Unit Holder Account Information and change of information (amendment)
- Customer Information and change of information
- Transactions
- Unit holder balance
- Consolidated inquiry
- Unit holder income distribution setup
- Balance view through various transaction screen (through hyper links)

Audit of personnel accessing the above data will stored/ logged and the details are as follows:

- User Identification
- Access date and Time (Application date and system date)
- Operation
- Function ID accessed
- Unit holder account/ Entity ID/ Auth rep ID
- Customer account
- To unit holder account (in case of transfers)
- To Customer account (in case of transfers)

The audit log process happens for the following New/ Modify/ Query/ Delete operations for a single record and fetch a single record from summary screen and view in detail screen. You can track actions in audit log in 'View' mode for a specific record for:

- UH and CIF – Tracks when user views specific record.
- Transaction – Tracks when specific transaction details is retrieved
- Queries/ Reports:
  - Consolidate Inquiry – Tracks when 'Investor Fund Balance' button is clicked for the retrieved UH Fund Balances
  - Unit Holder Balance – Tracks when specific Unit holder Balances is retrieved (this includes Balance view through various transaction screen by clicking 'View Balance' screen)

The system uses 'PIPA Audit log' as part of EOD activity to extract the data logged for the current day and for the module logged.

The multi record fetched through summary screen will not be logged; but a single record selected through the summary result will record the log.

You can fetch subscription records through summary screen by selecting a single record and view the record through detail screen.

Any data viewed via Detail screen by clicking Search/ Fetch button like List of values, find UH will not be logged by the system.

Note

All queries irrespective of success or unsuccessful output will be logged as part of audit requirement.

Following are the list of function IDs impacted in the system:

Function ID	Description	Audit against the Operations
UTDCUST	Customer Maintenance -> Detail	New/ Modify/ Query/ Delete/ Close/ Reopen
UTDCADD	CIF Address -> Detail	New/ Close/ Query/ Modify/ Reopen
UTDCFNMP	CIF Address Fund Map -> Detail	New/ Delete/ Close/ Authorise/ Query/ Reopen
UTDCIFLG	Customer Log -> Customer Log	New/ Query
UTDUH	Unit holder -> Detail	New/ Copy/ Query/ Modify/ Reopen
UTDUHBAL	Unit Holder Balances -> Summary	Enter Query
UTDUHCOE	Unit Holder Currency of Expression -> Detail	New/ Delete/ Close/ Authorise/ Query/ Reopen/ Modify
UTDUHDEL	Unit holder Deal -> Detail	New/ Delete/ Close/ Authorise/ Query/ Reopen/ Modify
UTDUHIDS	UH IDS Setup -> Detail	New/ Delete/ Close/ Authorise/ Query/ Reopen/ Modify
UTDUHIOF	UH IRRF Preference -> Detail	New/ Delete/ Close/ Authorise/ Query/ Reopen/ Modify
UTDUHLOI	UH LOI -> Detail	New/ Delete/ Close/ Authorise/ Query/ Reopen/ Modify
UTDUHNPI	UH NPI Preference -> Detail	New/ Delete/ Close/ Authorize/ Query/ Reopen/ Modify
UTDUHNTX	UH Non Tax Limits -> Detail	New/ Delete/ Close/ Authorise/ Query/ Reopen/ Modify
UTDUHPR	UH Portfolio Re Adjustment -> Detail	New/ Delete/ Close/ Authorize/ Query/ Reopen/ Modify

Function ID	Description	Audit against the Operations
UTDACCLS	UH Status Change -> Detail	New/ Delete/ Authorize/ Query/ Modify
UTDADJ02	Transaction -> Adjustment Sub-scription	New/ Delete/ Authorize/ Query/ Modify
UTDADJ03	Transaction -> Adjustment Redemption	New/ Delete/ Authorize/ Query/ Modify
UTDTXN01	Transaction -> IPO Subscription	New/ Delete/ Authorize/ Reverse Query/ Modify
UTDTXN02	Transaction -> Subscription	New/ Delete/ Authorize/ Reverse/ Query/ Modify
UTDTXN03	Transaction -> Redemption	New/ Delete/ Authorize/ Reverse/ Query/ Modify
UTDTXN04	Transaction -> Switch	New/ Delete/ Authorize/ Reverse/ Query/ Modify
UTDTXN05	Transaction -> Transfer	New/ Delete/ Authorize/ Reverse/ Query/ Modify
UTDTXN06	Transaction -> Block	New/ Delete/ Authorize/ Query/ Modify
UTDTXN07	Transaction -> Un-Block	New/ Delete/ Authorize/ Query/ Modify
UTDTXN08	Transaction -> Consolidation	New/ Delete/ Authorize/ Query/ Modify
UTDTXN09	Transaction -> Split	New/ Delete/ Authorize/ Query/ Modify
UTDTXN10	Transaction -> Reissue	New/ Delete/ Authorize/ Query/ Modify
UTDTXNEE	Transaction -> Enrich Exchange Rate	Query
UTDTXNLT	Transaction -> Light Weight Transaction	New/ Authorize/ View/ Query
UTDCNVTX	Transaction -> Conversion	New/ Delete/ Authorize/ Query/ Modify
UTDAMT06	Amount Block -> Detail	New/ Delete/ Authorise/ Query/ Modify
UTDAMT07	Amount Un-Block -> Detail	New/ Delete/ Authorise/ Query/ Modify
UTDCOMCL	Tax Compliance -> Classification	New/ Delete/ Authorise/ Query/ Modify

Function ID	Description	Audit against the Operations
UTDDCTRO	UH Dividend Component Override -> Detail	New/ Delete/ Authorise/ Query/ Modify
UTDFATMT	FATCA -> Entity FATCA Classification	New/ Delete/ Authorize/ Query/ Modify
UTDFNBAL	Investor fund Balance -> Summary	Query
UTDFNENT	Fund Entity -> Detail	New/ Delete/ Close/ Authorise/ Query/ Reopen/ Modify
UTDKYCCD	KYC Chasing Details -> Detail	New/ Delete/ Authorise/ Query/ Modify
UTDOLT	One Legged Transfer -> Detail	New/ Query
UTDPRQRY	Back Data Propagation -> Propagation Enquiry	Enter Query
UTDPRTXN	Back Data Propagation -> UT Transaction	New/ Delete/ Authorize/ Query/ Modify
UTDROPUT	Back Data Propagation -> UT Propagation	New/ Authorise/ Query
LEDPROSI	Back Data Propagation -> LEP Propagate SI	New/ Delete/ Authorize/ Query/ Modify
LEDPRTXN	Back Data Propagation -> LEP Transaction	New/ Delete/ Authorize/ Query/ Modify
UTDRTAIO	RTA Transfers -> Detail	New/ Query
UTDSCADH	Share Class Adhoc Conversion -> Detail	New/ Delete/ Close/ Authorise/ Query/ Modify/ Reopen
UTSCOINQ	Queries -> Consolidated Enquiry	View
LEDPLAN	LEP Online -> Policy	New/ Delete/ Close/ Authorise/ Query/ Reopen/ Modify
LEDPLCES	LEP Maintenance -> Policy Cession	New/ Delete/ Reverse/ Authorise/ Query/ Modify
LEDPLREV	LEP Online -> Policy Reversal	New/ Delete/ Authorise/ Query/ Modify
LEDPLSUR	LEP Online -> Policy Surrender	New/ Delete/ Reverse/ Authorise/ Query/ Modify
LEDPLSWI	LEP Online -> Policy Switch	New/ Delete/ Reverse/ Authorise/ Query/ Modify
LEDPLTOP	LEP Online -> Policy Top Up	New/ Delete/ Reverse/ Authorise/ Query/ Modify

Function ID	Description	Audit against the Operations
UTDATREP	Auth Rep Maintenance -> Detail	New/ Delete/ Authorise/ Query/ Modify
UTDENTMN	Single Entity Maintenance -> Detail	New/ Delete/ Authorise/ Query/ Modify

The SMTB_SMS_LOG and SMTBS_SMS_ACTION_LOG tables will log the audit information and hence the system will purge/ archive the data of these two data stores.

Note

After EOD, the system will store the audit logging details in PIPAAUDITPROCESSTBL. The purging will happen in PIPAAUDITPROCESSTBL table.

5. External System Maintenance

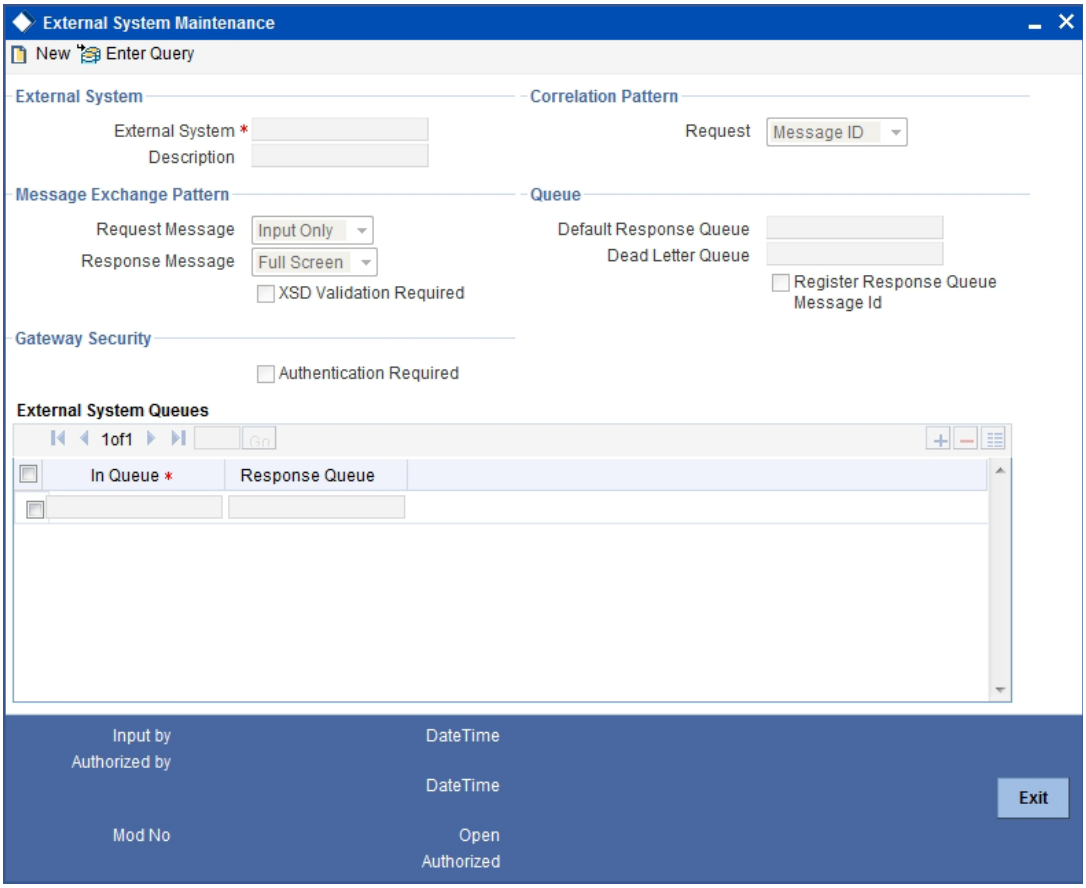
5.1 Introduction

Integration of different applications and solutions is a key area in today's systems. A variety of specialized applications deployed on disparate platforms and using different infrastructure need to be able to communicate and integrate seamlessly with FCIS, in order to exchange data. FCIS facilitates maintenance of such integration in the following screens:

- External System Maintenance
- External System Functions
- Message Media Maintenance
- Media Control System Maintenance

5.2 Maintaining External System

You need to maintain an external system that will communicate with FCIS. You can maintain and modify these parameters 'External System Maintenance' screen. You can invoke this screen by typing 'UTDEXSYS' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.



The various parameters that can be maintained in this screen are described below.

External System

You can maintain the following parameters here:

External System

Alphanumeric; 15 Characters; Mandatory

Specify a name for the external system. This should be the same as the Source in an incoming message.

Description

Alphanumeric; 35 Characters; Mandatory

Specify a brief description for the External System.

Correlation Pattern

You can maintain the following parameters here:

Request

Mandatory

Select a way in which the external system should correlate its request message with the response message, from the adjoining drop-down list. This list displays the following values:

- Message ID – Select if you want to use message ID of a request message as the Correlation ID in the corresponding response message.
- Correlation ID – Select if you want to maintain Correlation ID of a request message as the Correlation ID of the corresponding response message.

Message Exchange Pattern

You can maintain the following parameters here:

Request Message

Mandatory

Select a pattern for the generated request message from the adjoining drop-down list. This list displays the following values:

- Full Screen – Select if you want to view the full screen of the request message.
- Input Only – Select if you want to view only the input of the request message.

Note

If you select ‘Full Screen’ as the request message, the response message will also display ‘Full Screen’.

Response Message

Mandatory

Select a pattern for the generated response message from the adjoining drop-down list. This list displays the following values:

- Full Screen – Select if you have selected ‘Full Screen’ for the request message.
- Record Identification Msg – Select if you have selected ‘Input Only’ for the request message.

Queue

You can maintain the following parameters here:

Default Response Queue

Alphanumeric; 105 Characters; Optional

Specify a valid response queue name as the default response queue, for each of the 'In Queue' through which the External System will communicate with FCIS.

Dead Letter Queue

Alphanumeric; 105 Characters; Optional

Specify a valid queue as dead letter queue to direct the received messages which are non-readable.

Note

If the Dead Letter Queue is not defined, such messages will be redirected to a queue with the name of the request queue appended with '_E'.

XSD Validation Required

Optional

Check this box if you want to validate the request message against its corresponding XSD.

Register Response Queue Message ID

Optional

Check this box if you want to log the message ID, which is provided by the Response Queue, when a response message is posted into the queue.

External System Queues

You can maintain the following parameters here:

In Queue

Alphanumeric; 105 Characters; Mandatory

Specify the name of the queue from which the messages were received. The name of the queue will help identify the external system.

Note

- This is required only if an incoming message does not display the source of the message. An In Queue is mapped to only one External System.
- You can map multiple queues to a source. System will allow a source to post messages to multiple queues.

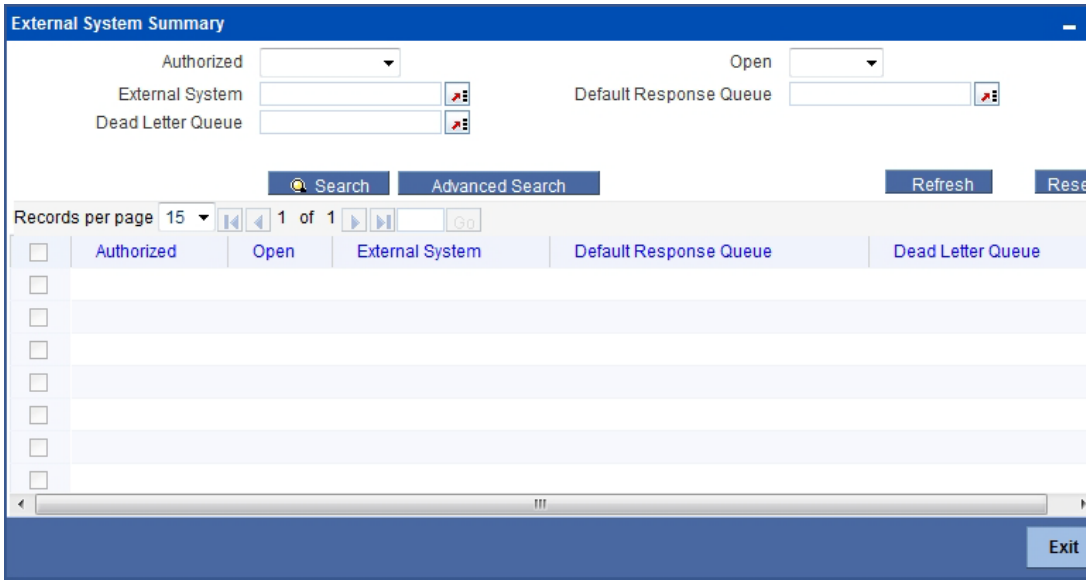
Response Queue

Alphanumeric; 105 Characters; Mandatory

Specify a valid response queue to display the queue name on posting a request message into the In Queue, when the External System fails. Response queue can be maintained for every In Queue.

5.3 Retrieving External System Details

You can view, modify, delete and authorize External system details in the 'External System Summary' screen. You can invoke this screen by typing 'UTSEXSYS' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



You can perform the following actions using this screen

5.3.1 Viewing External System Details

You can view previously entered details of external system in the 'External System Summary' screen, as follows:

- Specify any or all of the following details in the 'External System Summary' screen:
  - The status of the record in the Authorization Status field. If you choose the 'Blank Space' option, then all the records that involve the specified External System are retrieved.
  - The status of the record in the Open field. If you choose the 'Blank Space' option, then all the records that involve the specified External System are retrieved.
  - External System
  - Default Response Queue
  - Dead Letter Queue

Click 'Search' button to view the records. All records with the specified details are retrieved and displayed in the lower portion of the screen.

You can also search the record by using combination of % and alphanumeric value.

5.3.2 Deleting External System Details

You can delete only unauthorized records in the system. To delete a record that you have previously entered:

- Invoke the 'External System Summary' screen from the Browser.
- Select the status of the record that you want to retrieve for deletion.
- Specify any or all of the details and click 'Search' button. All records with the specified details are retrieved and displayed in the lower portion of the screen.

- Double click the record that you want to delete. The ‘External System Maintenance’ screen is displayed.
- Select Delete operation from the Action list. The system prompts you to confirm the deletion, and the record is deleted physically from the system database.

5.3.3 Modifying External System Details

You can modify only unauthorized records in the system. To modify a record that you have previously entered:

- Invoke the ‘External System Summary’ screen from the Browser.
- Select the status of the record that you want to retrieve for modification.
- Specify any or all of the details and click ‘Search’ button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to modify. The ‘External System Maintenance’ screen is displayed.
- Select Edit operation from the Action list and modify the details. After modifying the details, click Save to save the modifications.

You can edit External System details as many times as necessary before you authorize it.

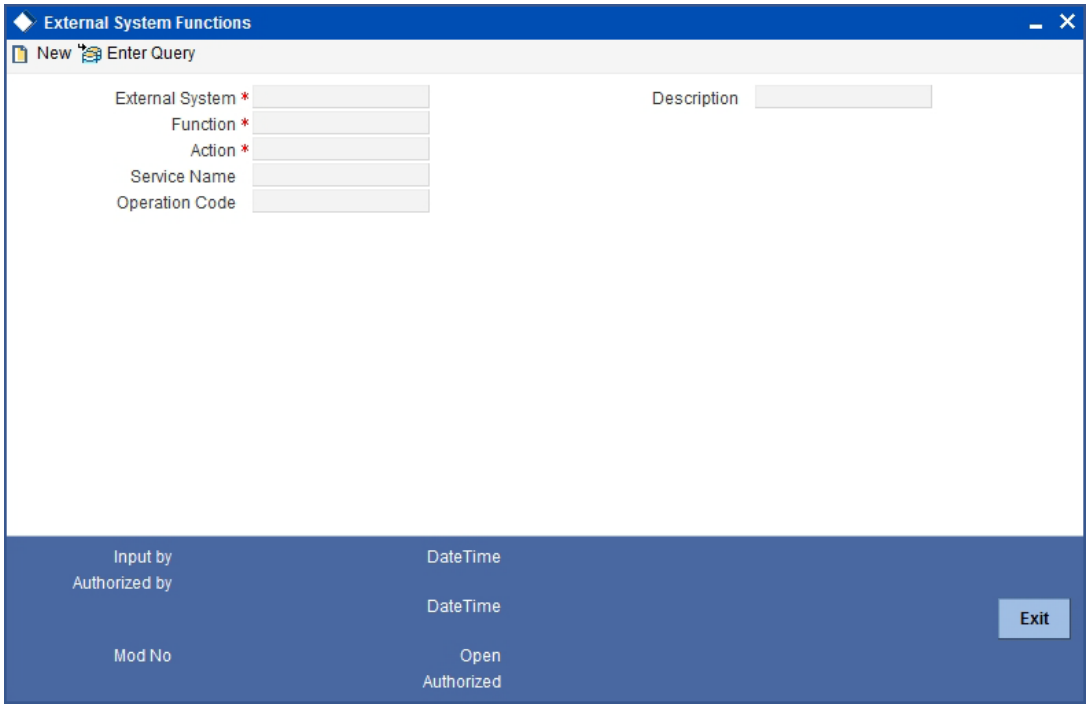
5.3.4 Authorizing External System Details

You can authorize records in the system. To authorize a record that you have previously entered:

- Invoke the ‘External System Summary’ screen from the Browser.
- Select the status of the record that you want to retrieve for authorization.
- Specify any or all of the details and click ‘Search’ button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to authorize. The ‘External System Maintenance’ screen is displayed.
- Select authorize operation from the Action list. The system prompts you to confirm the authorization, and the record is authorized.

5.4 Maintaining External System Functions

You can define access rights to an external system using the ‘External System Functions’ screen. You can invoke this screen by typing ‘UTDEXFUN’ in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.



You can specify the following details:

External System

Alphanumeric; 15 Characters; Mandatory

Specify an external system for which you wish to provide access rights from the adjoining option list. The adjoining option list displays all the external systems you have maintained at the ‘External Systems Maintenance’ level.

Description

Alphanumeric; 105 Characters; Mandatory

Description of the specified external system is defaulted here.

Function ID

Alphanumeric; 8 Characters; Mandatory

Specify a valid function ID from the adjoining option list. The function IDs are invoked from Gateway Functions.

Action

Alphanumeric; 10 Characters; Mandatory

Select an action for the external system from the adjoining option list.

Service Name

Alphanumeric; 50 Characters; Optional

Service name is defaulted here based on the specified Function ID and Action.

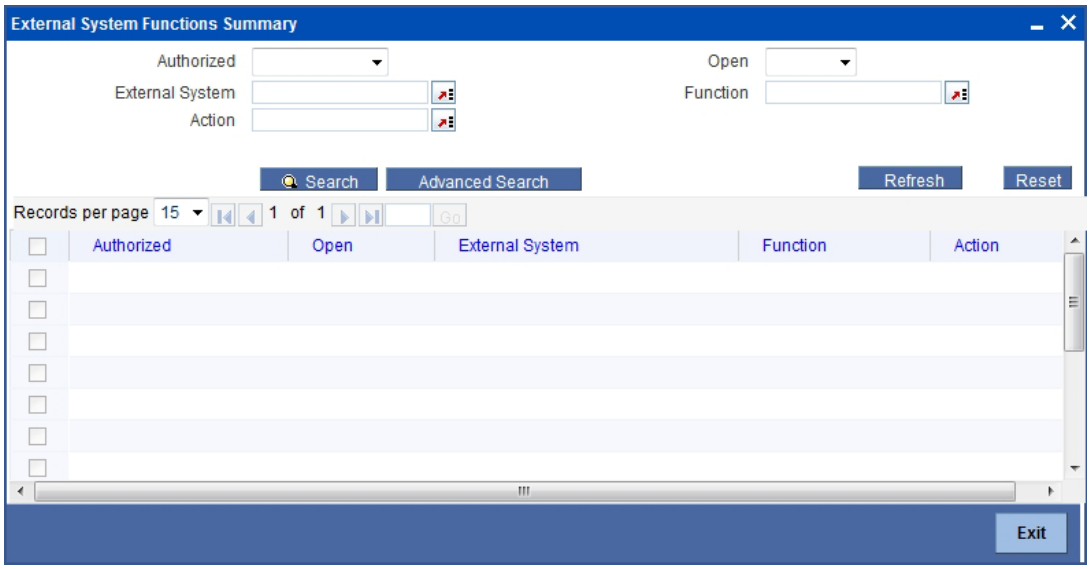
Operation Code

Alphanumeric; 50 Characters; Optional

Operation Code is defaulted here based on the specified Function ID and Action.

5.5 Retrieving External System Details

You can view, modify, delete and authorize external system function details in the 'External System Functions Summary' screen. You can invoke this screen by typing 'UTSEXFUN' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



You can perform the following actions using this screen

5.5.1 Viewing External System Functions Details

You can view previously entered details of external system in the 'External System Functions Summary' screen, as follows:

- Specify any or all of the following details in the 'External System Functions Summary' screen:
  - The status of the record in the Authorization Status field. If you choose the 'Blank Space' option, then all the records that involve the specified External System Functions are retrieved.
  - The status of the record in the Open field. If you choose the 'Blank Space' option, then all the records that involve the specified External System Functions are retrieved.
  - External System
  - Function
  - Action

Click 'Search' button to view the records. All records with the specified details are retrieved and displayed in the lower portion of the screen.

You can also search the record by using combination of % and alphanumeric value.

5.5.2 Deleting External System Functions Details

You can delete only unauthorized records in the system. To delete a record that you have previously entered:

- Invoke the 'External System Functions Summary' screen from the Browser.
- Select the status of the record that you want to retrieve for deletion.
- Specify any or all of the details and click 'Search' button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to delete. The 'External System Functions Maintenance' screen is displayed.
- Select Delete operation from the Action list. The system prompts you to confirm the deletion, and the record is deleted physically from the system database.

5.5.3 Modifying External System Function Details

You can modify only unauthorized records in the system. To modify a record that you have previously entered:

- Invoke the 'External System Functions Summary' screen from the Browser.
- Select the status of the record that you want to retrieve for modification.
- Specify any or all of the details and click 'Search' button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to modify. The 'External System Functions Maintenance' screen is displayed.
- Select Edit operation from the Action list and modify the details. After modifying the details, click Save to save the modifications.

You can edit External System details as many times as necessary before you authorize it.

5.5.4 Authorizing External System Function Details

You can authorize records in the system. To authorize a record that you have previously entered:

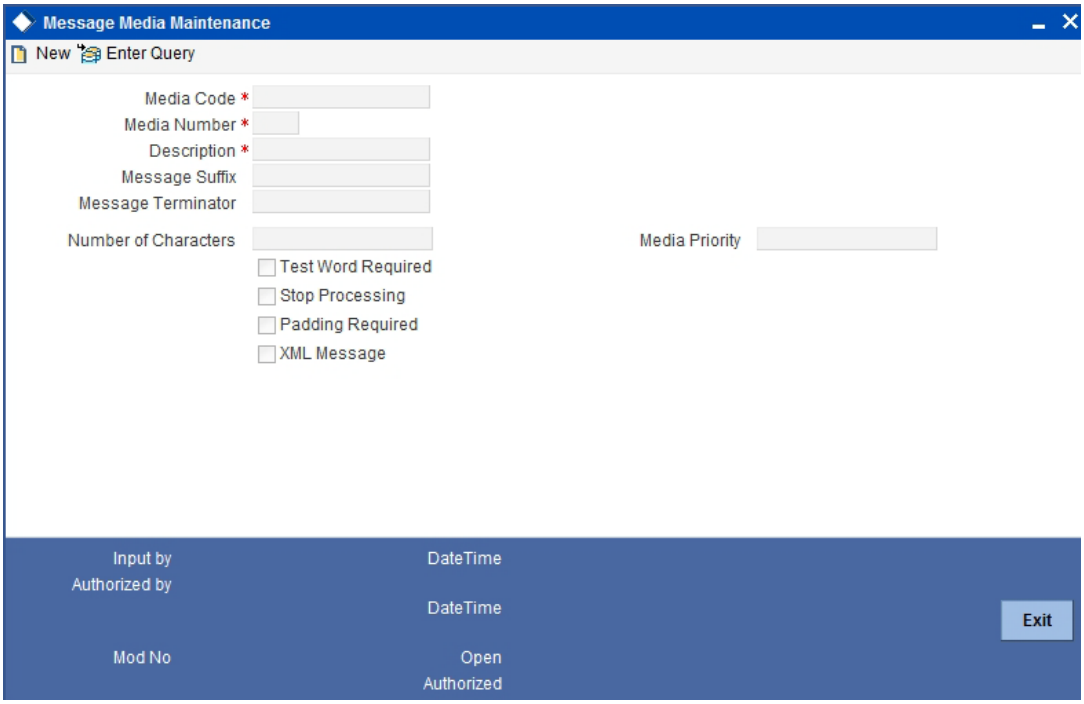
- Invoke the 'External System Functions Summary' screen from the Browser.
- Select the status of the record that you want to retrieve for authorization.
- Specify any or all of the details and click 'Search' button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to authorize. The 'External System Functions Maintenance' screen is displayed.
- Select authorize operation from the Action list. The system prompts you to confirm the authorization, and the record is authorized.

5.6 Maintaining Message Media

FCIS facilitates maintenance of different media through which advices and messages can be generated. At your bank, you can only receive or route messages through a media that you have maintained in this screen. These specifications can be made only at the main branch and will be applicable to all the branches of your bank.

You can maintain standard media like Mail, Telex and SWIFT and also other media like CHIPS or any other country or customer specific media from which the messages will be routed. You can invoke the 'Message Media Maintenance' screen by typing 'UTDMEDIA' in

the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button



In this screen, you can maintain the following:

- The media types that can be used to transmit messages from and to your bank
- The compatible media for the media type you are maintaining

Media Code

Alphanumeric; 15 Characters; Mandatory

Specify a unique code to identify the media.

When you want to transit a message through a particular media type, you just have to specify the code assigned to the media type. The message will be routed automatically through the media.

Media Number

Numeric; 15 Characters; Mandatory

Specify a unique number with which you want to represent the media.

Description

Alphanumeric; 35 Characters; Mandatory

Specify description for the specified media code. The description will help you identify the code that it represents.

Message Suffix

Alphanumeric; 200 Characters; Optional

Specify padding characters which you want to add to the end of every outgoing message, automatically. The specified padding characters will be inserted, automatically, at the end of every outgoing message in the media.

Message Terminator

Alphanumeric; 100 characters; Optional

Specify padded characters that mark the end of the incoming messages in a media. The system identifies the end of an incoming message, in a file containing several messages, when it encounters the padding characters that you have specified for a media type.

Number of Characters

Numeric; 3 Characters; Optional

Specify the number of times you want to repeat the set of specified padding characters, if you opted to suffix an outgoing message with a set of padding characters.

The padding characters will be suffixed to every outgoing message in the media as many times as you specify.

Media Priority

Numeric; 2 Characters; Mandatory

Specify usage priority for each media type that you maintain. When dispatching messages to customers, the media type used for sending the message will be the one that is higher on the priority rating.

Test Word Required

Optional

Check this option if you want to insert the test word to the telex message manually before it is generated from your branch.

Stop Processing

Optional

Check this box if you want to stop the processing for the incoming and outgoing messages.

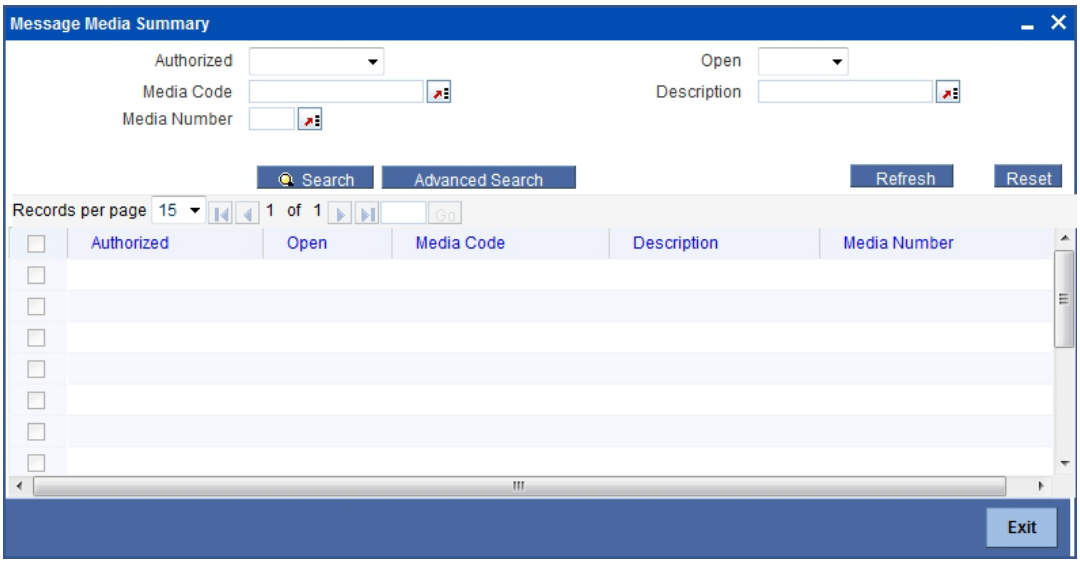
Padding Required

Optional

Check this box if you want to add the suffix to the outgoing messages.

5.7 Retrieving Message Media Details

You can view, modify, delete and authorize external system function details in the ‘Message Media Summary’ screen. You can invoke this screen by typing ‘UTSMEDIA’ in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



You can perform the following actions using this screen

5.7.1 Viewing Message Media Details

You can view previously entered details of external system in the ‘Message Media Summary’ screen, as follows:

- Specify any or all of the following details in the ‘Message Media Summary’ screen:
  - The status of the record in the Authorization Status field. If you choose the ‘Blank Space’ option, then all the records that involve the specified Message Media are retrieved.
  - The status of the record in the Open field. If you choose the ‘Blank Space’ option, then all the records that involve the specified Message Media are retrieved.
  - Media Code
  - Description
  - Media Number

Click ‘Search’ button to view the records. All records with the specified details are retrieved and displayed in the lower portion of the screen.

You can also search the record by using combination of % and alphanumeric value.

5.7.2 Deleting Message Media Details

You can delete only unauthorized records in the system. To delete a record that you have previously entered:

- Invoke the ‘Message Media Summary’ screen from the Browser.
- Select the status of the record that you want to retrieve for deletion.
- Specify any or all of the details and click ‘Search’ button. All records with the specified details are retrieved and displayed in the lower portion of the screen.

- Double click the record that you want to delete. The ‘Message Media Maintenance’ screen is displayed.
- Select Delete operation from the Action list. The system prompts you to confirm the deletion, and the record is deleted physically from the system database.

5.7.3 Modifying Message Media Details

You can modify only unauthorized records in the system. To modify a record that you have previously entered:

- Invoke the ‘Message Media Summary’ screen from the Browser.
- Select the status of the record that you want to retrieve for modification.
- Specify any or all of the details and click ‘Search’ button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to modify. The ‘Message Media Maintenance’ screen is displayed.
- Select Edit operation from the Action list and modify the details. After modifying the details, click Save to save the modifications.

You can edit External System details as many times as necessary before you authorize it.

5.7.4 Authorizing Message Media Details

You can authorize records in the system. To authorize a record that you have previously entered:

- Invoke the ‘Message Media Summary’ screen from the Browser.
- Select the status of the record that you want to retrieve for authorization.
- Specify any or all of the details and click ‘Search’ button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to authorize. The ‘Message Media Maintenance’ screen is displayed.
- Select authorize operation from the Action list. The system prompts you to confirm the authorization, and the record is authorized.

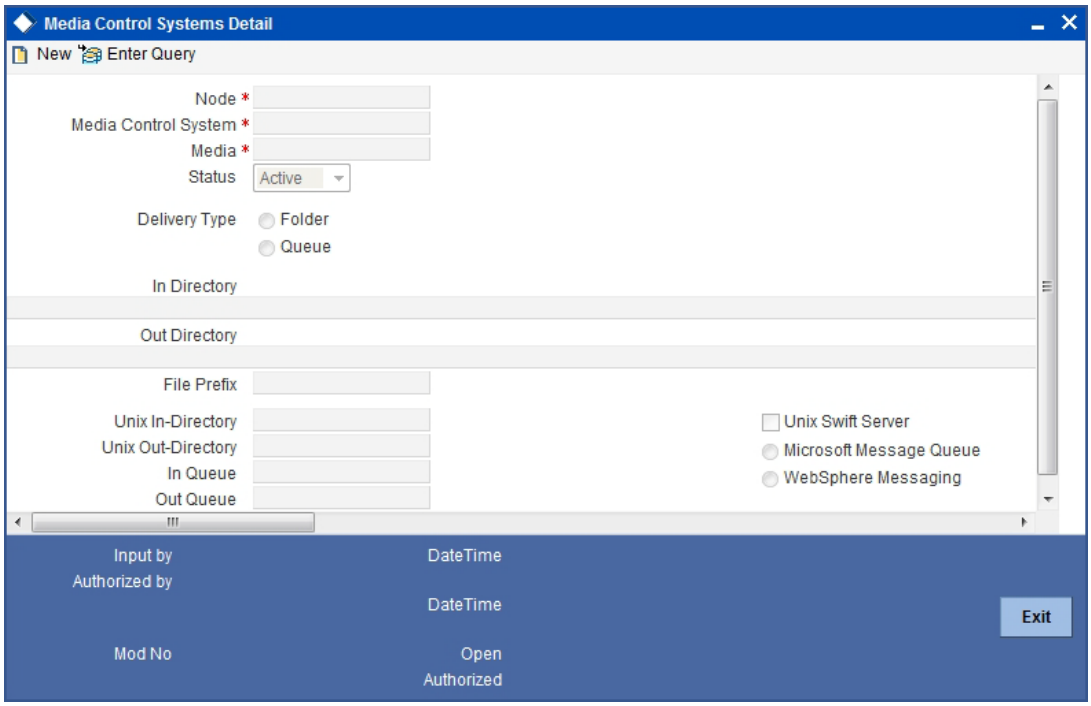
5.8 Maintaining Media Control System

The messages that are sent from and delivered to your bank are transmitted and received over sources that are external to FCIS. We shall call these external sources Media Control Systems (MCS).

In a distributed environment, the database of a branch is located in a node or server. The MCS of the messages are also installed in a node. Thus, while defining an MCS, you also need to indicate the node in which it is installed.

An MCS can handle only one media, hence you need to set up several media control systems for the various media types maintained for your bank. Apart from indicating the media type for an MCS, you can also indicate separate directories from which FCIS should read and write incoming and outgoing messages, for a given media.

You can invoke ‘Media Control System Maintenance’ screen by typing ‘UTDMCS’ in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



You can maintain the following parameters here:

Node

Alphanumeric; 3 Characters; Mandatory

Specify a node or server at which the MCS is located, from the adjoining option list. A node is the Database instance on which FCIS is installed. A branch’s database is located in a node and an MCS is also installed in a node.

Media Control System

Alphanumeric; 15 Characters; Mandatory

Specify a unique code for MCS to identify the external source. You can follow your own convention for devising this code.

Media

Alphanumeric; 15 Characters; Mandatory

Specify the media for which your bank is using the MCS, from the adjoining option list. The option-list displays the media codes maintained at the ‘Message Media Maintenance’ level.

Status

Mandatory

Select a valid status of an MCS from the adjoining drop-down list. This list displays the following values:

- Active – Select if you want to direct the messages through MCS.
- Passive – Select if you do not want to direct any message to through MCS. If the status of MCS is passive, then FCIS will not write into or read from the directories on the node.

Delivery Type

Mandatory

Select a valid type of delivery from the options. The following options are available for selection:

- Folder – If you select this option, you must specify the ‘In Directory’ and ‘Out Directory’ for Windows Server. Further, after selecting this option, if you check the option ‘Unix Swift Server’ for a UNIX SWIFT server, then you must specify the ‘Unix In-Directory’ and the ‘Unix Out-Directory’.
- Queue – If you select this option, you must specify ‘In Queue’, ‘Out Queue’ and select a valid type of queue from the options. The following options are available for selection:
  - Microsoft Message Queue – Select if you want to maintain Microsoft message queue.
  - WebSphere Messaging Queue – Select if you want to maintain WebSphere message queue.

In Directory

Alphanumeric; 100 Characters; Optional

Specify the full path of the directory from which FCIS should read and write incoming message, if you have maintained the Delivery Type as ‘Folder' and the SWIFT server as Windows server.

Out Directory

Alphanumeric; 100 Characters; Optional

Specify the full path of the directory from which FCIS should read and write outgoing message, if you have maintained the Delivery Type as ‘Folder' and the SWIFT server as Windows server.

File Prefix

Alphanumeric; 1 Character; Optional

Specify a unique identifier for the specified MCS to identify the outgoing message files generated in a different media.

Unix-In-Directory

Alphanumeric; 100 Characters; Optional

Specify the full path of the directory on the SWIFT server where you would like to store incoming SWIFT message hand-off files. The system will pickup and process all incoming SWIFT message files from this directory.

Unix-Out-Directory

Alphanumeric; 100 Characters; Optional

Specify the full path of the directory on the SWIFT server where you would like to store outgoing SWIFT message hand-off files.

In Queue

Alphanumeric; 100 Characters; Optional

Specify the full path of the queue in the node or server into which the MCS should store the incoming message hand-off file, if the Delivery type is Queue. The system will pickup and read all incoming messages transmitted through the specified media from this queue, by default

Out Queue

Alphanumeric; 100 Characters; Optional

Specify the full path of the queue in the node or server into which the message hand-off file from the system, for the specified media, should be stored. The MCS, which is also located on the same node, will store the outgoing messages in this queue by default.

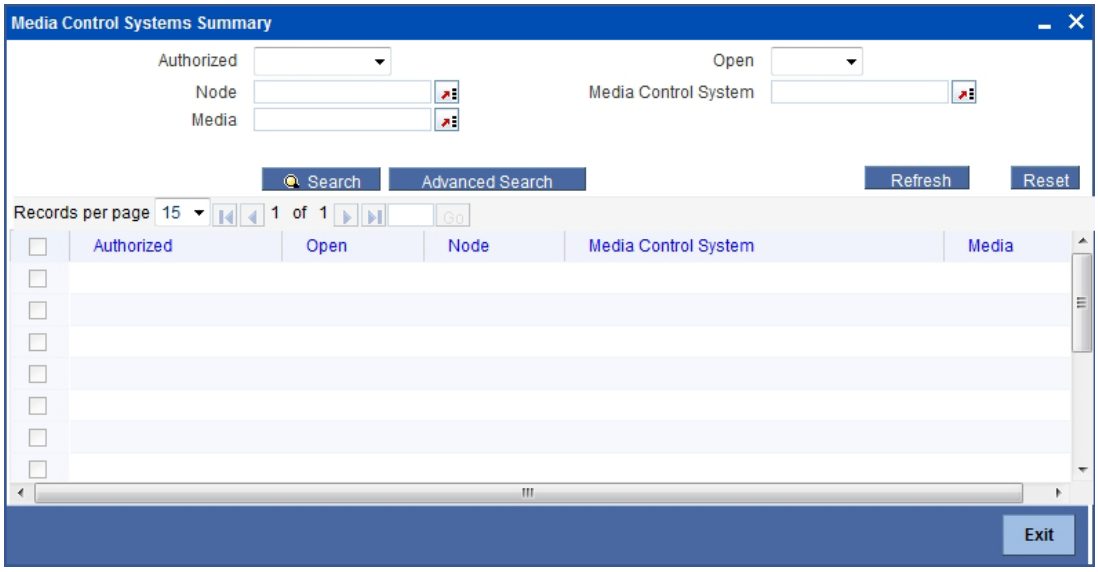
Unix Swift Server

Optional

Check this box if the SWIFT server at your Bank is on UNIX.

5.9 Retrieving Media Control System Details

You can view, modify, delete and authorize external system function details in the 'Media Control System Summary' screen. You can invoke this screen by typing 'UTSMCS' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



You can perform the following actions using this screen.

5.9.1 Viewing Media Control System Details

You can view previously entered details of external system in the 'Media Control System Summary' screen, as follows:

- Specify any or all of the following details in the 'Media Control System Summary' screen:
  - The status of the record in the Authorization Status field. If you choose the 'Blank Space' option, then all the records that involve the specified Media Control System are retrieved.
  - The status of the record in the Open field. If you choose the 'Blank Space' option, then all the records that involve the specified Media Control System are retrieved.
  - Node
  - Media Control System
  - Media

Click 'Search' button to view the records. All records with the specified details are retrieved and displayed in the lower portion of the screen.

You can also search the record by using combination of % and alphanumeric value.

5.9.2 Deleting Media Control System Details

You can delete only unauthorized records in the system. To delete a record that you have previously entered:

- Invoke the 'Media Control System Summary' screen from the Browser.
- Select the status of the record that you want to retrieve for deletion.
- Specify any or all of the details and click 'Search' button. All records with the specified details are retrieved and displayed in the lower portion of the screen.

- Double click the record that you want to delete. The ‘Media Control System Maintenance’ screen is displayed.
- Select Delete operation from the Action list. The system prompts you to confirm the deletion, and the record is deleted physically from the system database.

5.9.3 Modifying Media Control System Details

You can modify only unauthorized records in the system. To modify a record that you have previously entered:

- Invoke the ‘Media Control System Summary’ screen from the Browser.
- Select the status of the record that you want to retrieve for modification.
- Specify any or all of the details and click ‘Search’ button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to modify. The ‘Media Control System Maintenance’ screen is displayed.
- Select Edit operation from the Action list and modify the details. After modifying the details, click Save to save the modifications.

You can edit External System details as many times as necessary before you authorize it.

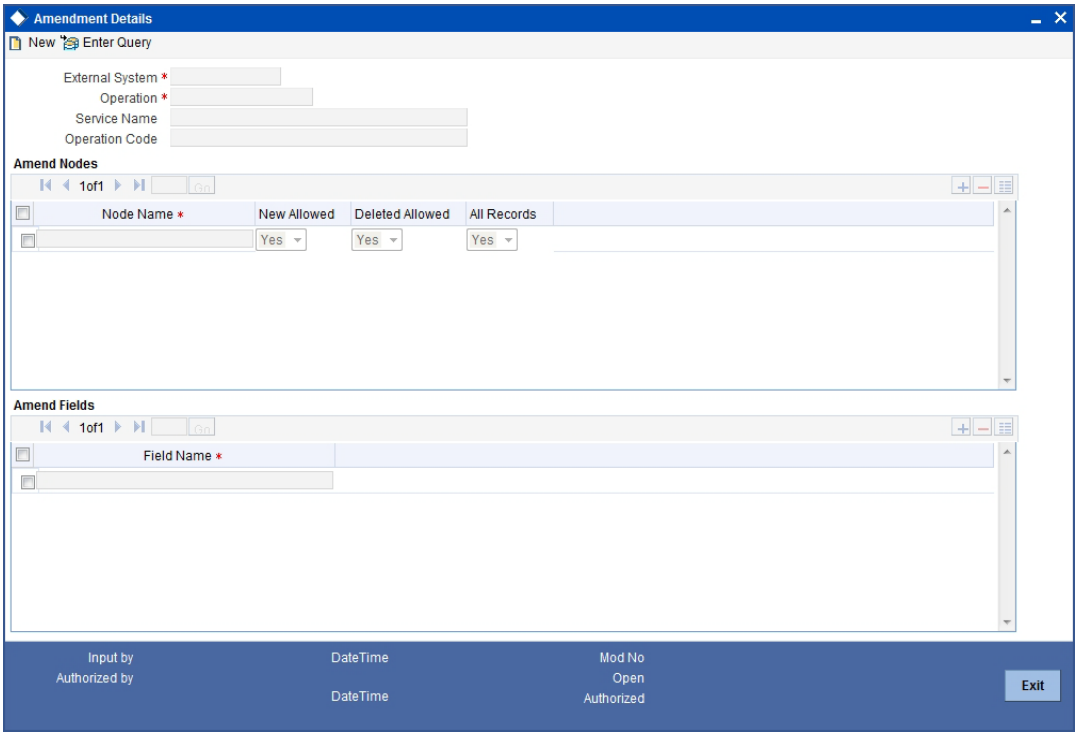
5.9.4 Authorizing Media Control System Details

You can authorize records in the system. To authorize a record that you have previously entered:

- Invoke the ‘Media Control System Summary’ screen from the Browser.
- Select the status of the record that you want to retrieve for authorization.
- Specify any or all of the details and click ‘Search’ button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to authorize. The ‘Media Control System Maintenance’ screen is displayed.
- Select authorize operation from the Action list. The system prompts you to confirm the authorization, and the record is authorized.

5.10 Maintaining Amendment Details

FCIS facilitates maintenance of nodes and fields which are amended through external system. You can invoke this screen by typing UTDAMDMT in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.



You can maintain the following parameters here:

External System

Alphanumeric; 15 Characters; Mandatory

Select an external system for which amendable maintenance is done, from the adjoining option list.

Operation

Alphanumeric; Mandatory

Specify the Gateway operation for which Amendable maintenance is done.

Service Name

Alphanumeric; 50 Characters; Optional

Select the service name for which amendable maintenance is done, from the adjoining option list.

Operation Code

Alphanumeric; 50 Characters; Optional

Select the operation code from the adjoining option list.

Amend Nodes

Node Name

Specify the name of the node which can be amended through external system. The adjoining option list displays the list of nodes.

New Allowed

New Allowed indicates whether new records can be added in the node.

Deleted Allowed

Delete Allowed indicates whether existing records can be deleted from the node.

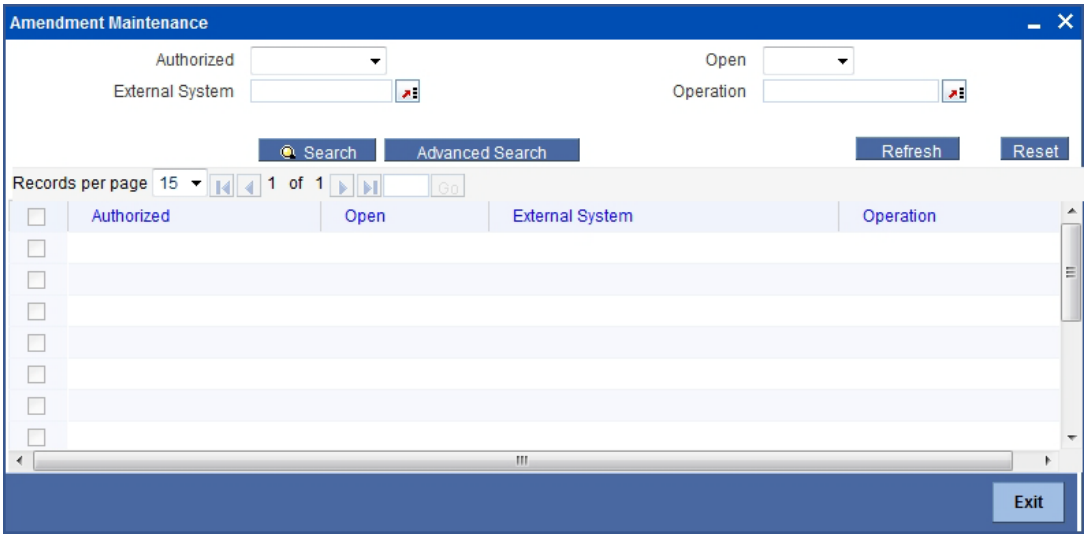
Amend Fields

Field Name

Specify the field name which can be amended through external system. The adjoining option list displays the list of the fields in the node.

5.11 Retrieving Amendment Details

You can view, modify, delete and authorize external system details in the 'Amendment Maintenance Summary' screen. You can invoke this screen by typing 'UTSAMDMT' in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



You can perform the following actions using this screen.

5.11.1 Viewing Amendment Details

You can view previously entered details of external system in the 'Amendment Maintenance Summary' screen, as follows:

- Specify any or all of the following details in the 'Amendment Maintenance Summary' screen:
  - The status of the record in the Authorization Status field. If you choose the 'Blank Space' option, then all the records that involve the specified External System are retrieved.
  - The status of the record in the Open field. If you choose the 'Blank Space' option, then all the records that involve the specified External System are retrieved.
  - External System
  - Operation

Click 'Search' button to view the records. All records with the specified details are retrieved and displayed in the lower portion of the screen.

You can also search the record by using combination of % and alphanumeric value.

5.11.2 Deleting Amendment Details

You can delete only unauthorized records in the system. To delete a record that you have previously entered:

- Invoke the 'Amendment Maintenance Summary' screen from the Browser.
- Select the status of the record that you want to retrieve for deletion.
- Specify any or all of the details and click 'Search' button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to delete. The 'Amendment Details' screen is displayed.
- Select Delete operation from the Action list. The system prompts you to confirm the deletion, and the record is deleted physically from the system database.

5.11.3 Modifying Amendment Details

You can modify only unauthorized records in the system. To modify a record that you have previously entered:

- Invoke the 'Amendment Maintenance Summary' screen from the Browser.
- Select the status of the record that you want to retrieve for modification.
- Specify any or all of the details and click 'Search' button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to modify. The 'Amendment Details' screen is displayed.
- Select Edit operation from the Action list and modify the details. After modifying the details, click Save to save the modifications.

You can edit External System details as many times as necessary before you authorize it.

5.11.4 Authorizing Amendment Details

You can authorize records in the system. To authorize a record that you have previously entered:

- Invoke the 'Amendment Maintenance Summary' screen from the Browser.
- Select the status of the record that you want to retrieve for authorization.
- Specify any or all of the details and click 'Search' button. All records with the specified details are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to authorize. The 'Amendment Details' screen is displayed.
- Select authorize operation from the Action list. The system prompts you to confirm the authorization, and the record is authorized.

6. Function ID Glossary

S

Security User Guide
May 2018
Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India
Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax:+91 22 6718 3001
www.oracle.com/financialservices/