Security User Guide

Oracle FLEXCUBE Investor Servicing

Release 14.7.0.1.0
Part Number F71715-01

May 2023

ORACLE

Security User Guide
May 2023
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/

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	Description
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

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.

This chapter contains the following sections:

2.1 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

2.2 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.

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.

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.

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.

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.

2.3 Other Features of Security Management System

This section contains the following topics:

2.3.1 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.

2.3.2 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.

2.3.3 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.

2.3.4 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.

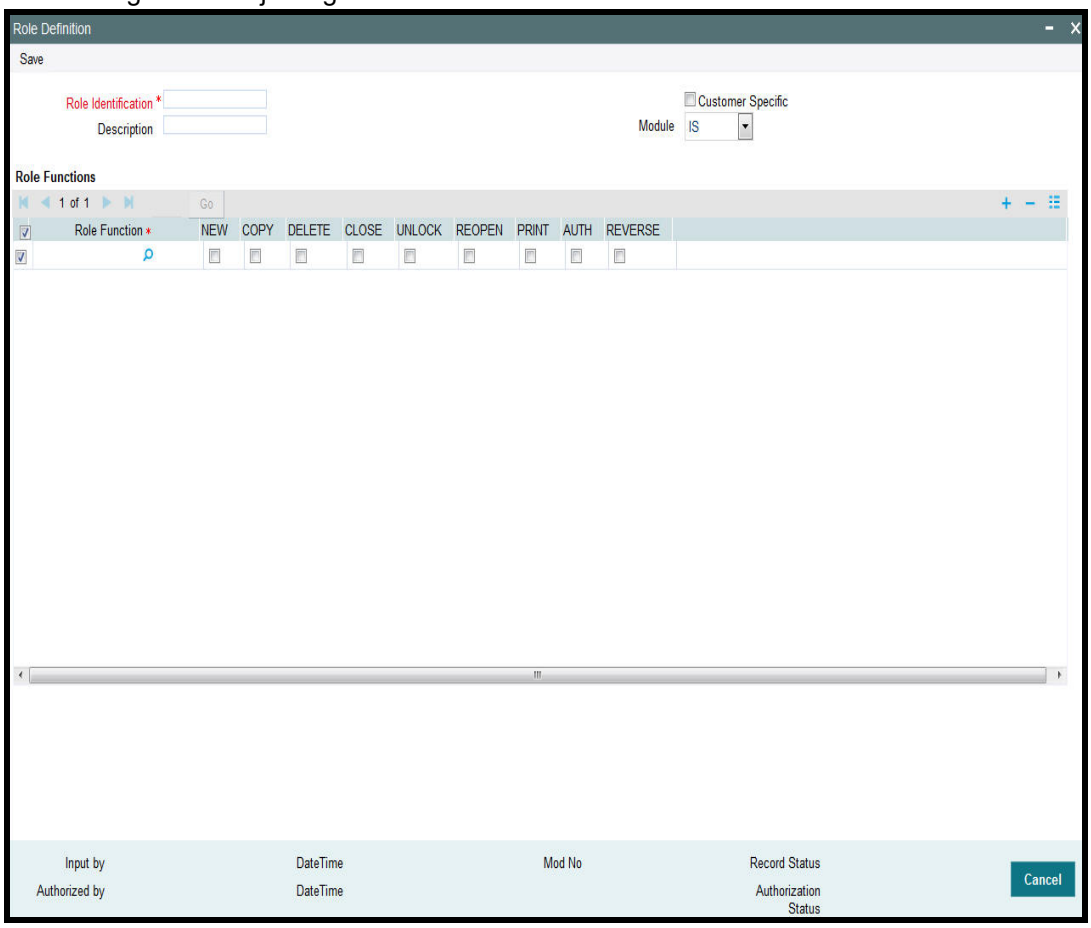
2.4 Role Profiles

This section contains the following topics:

- Section 2.4.7, "Editing Role Profile"

2.4.1 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.



Role Identification

Alphanumeric, 15 Characters; Mandatory

Specify a unique identifier for the role profile.

Description

Alphanumeric, 35 Characters; Optional

Specify 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 from the drop-down list. The list displays the following values:

- IS
- Corporate

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.

Role Function

Alphanumeric; 8 Characters; Mandatory

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:

2.4.1.1 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)
- Reverse (Reverse the details of selected records)

2.4.1.2 Contracts and On-line Transaction Processing

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

2.4.1.3 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.

2.4.2 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.

2.4.3 Copying Role Profile of Existing Role

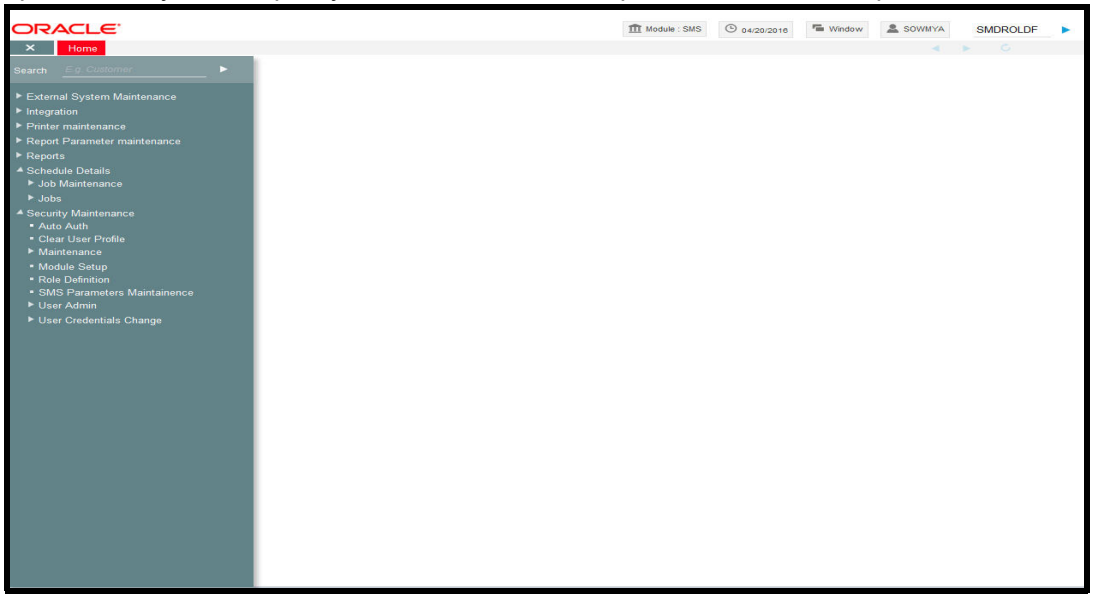
Often, you may have to create a Role Profile that closely resembles an existing one. In such a case, you can copy the existing profile on to the new one.

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.

2.4.4 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:

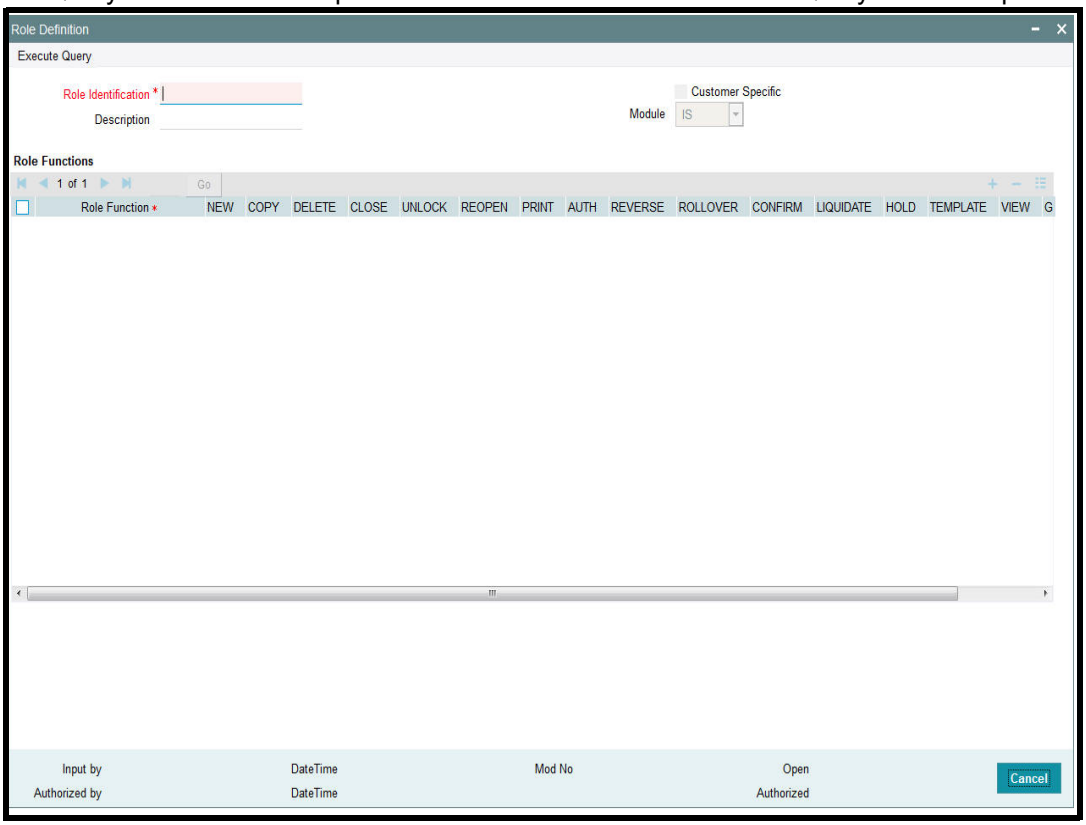
- Click the F7 button
- Input the Role ID
- Click on F8

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.

2.4.5 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.

2.4.6 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.

2.4.7 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.

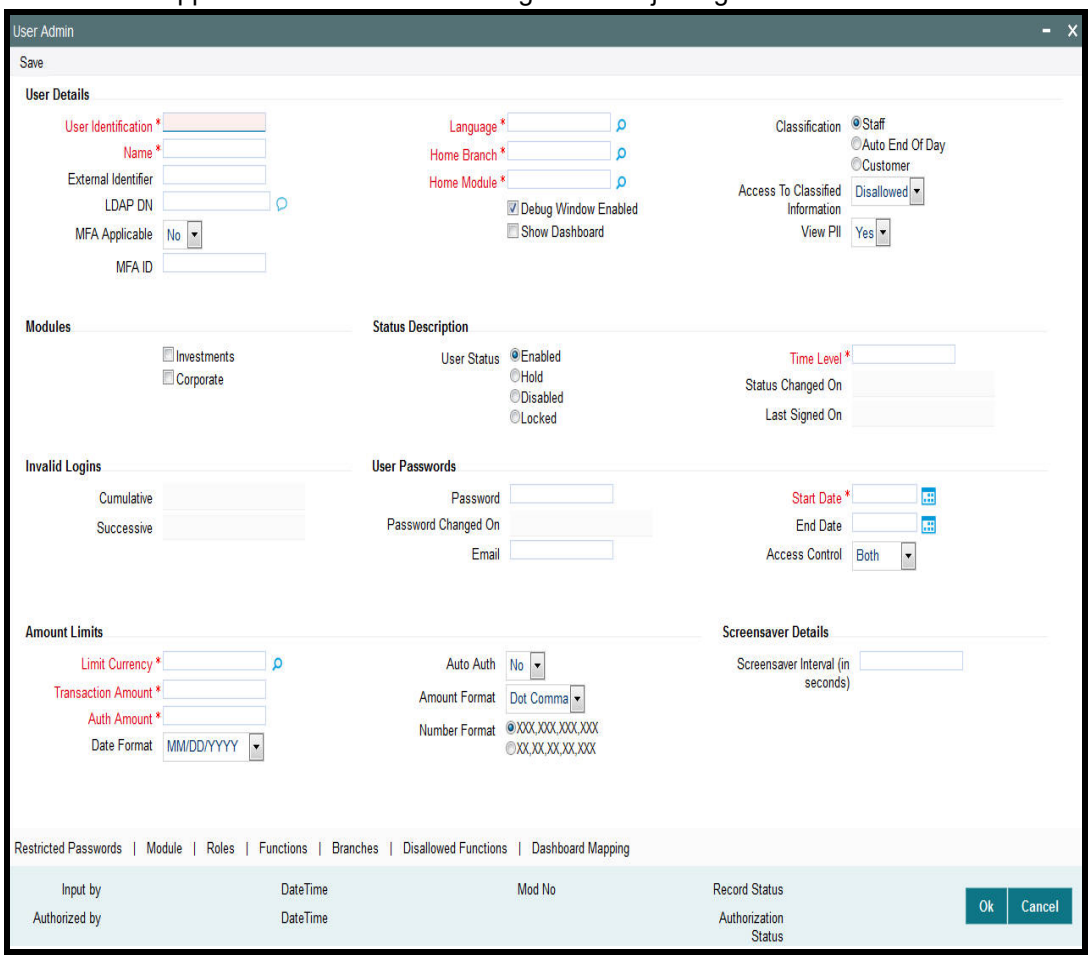
2.5 User Profile

This section contains the following topics:

2.5.1 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.



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.

Four SSO types SAML, TOKEN, IDCS_TOKEN and DEFAULT are currently supported in FCIS. For setting up FCIS to support SSO, Kindly refer FCIS_Property_File_Creation.pdf.

MFA Applicable

Optional

Select if Multi Factor Authorization (MFA) is applicable or not from the drop-down list. The list displays the following values:

- Yes
- No

MFA ID

Alphanumeric; 50 Characters; Optional

Specify the multi factor authorization ID.

If 'MFA Applicable' field is selected as 'Yes', then 'MFA ID' is mandatory.

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:

User	Description
Staff	A user of the system who is an employee of your 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 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.

Successive

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
- MM/DD/YYYY
- 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:

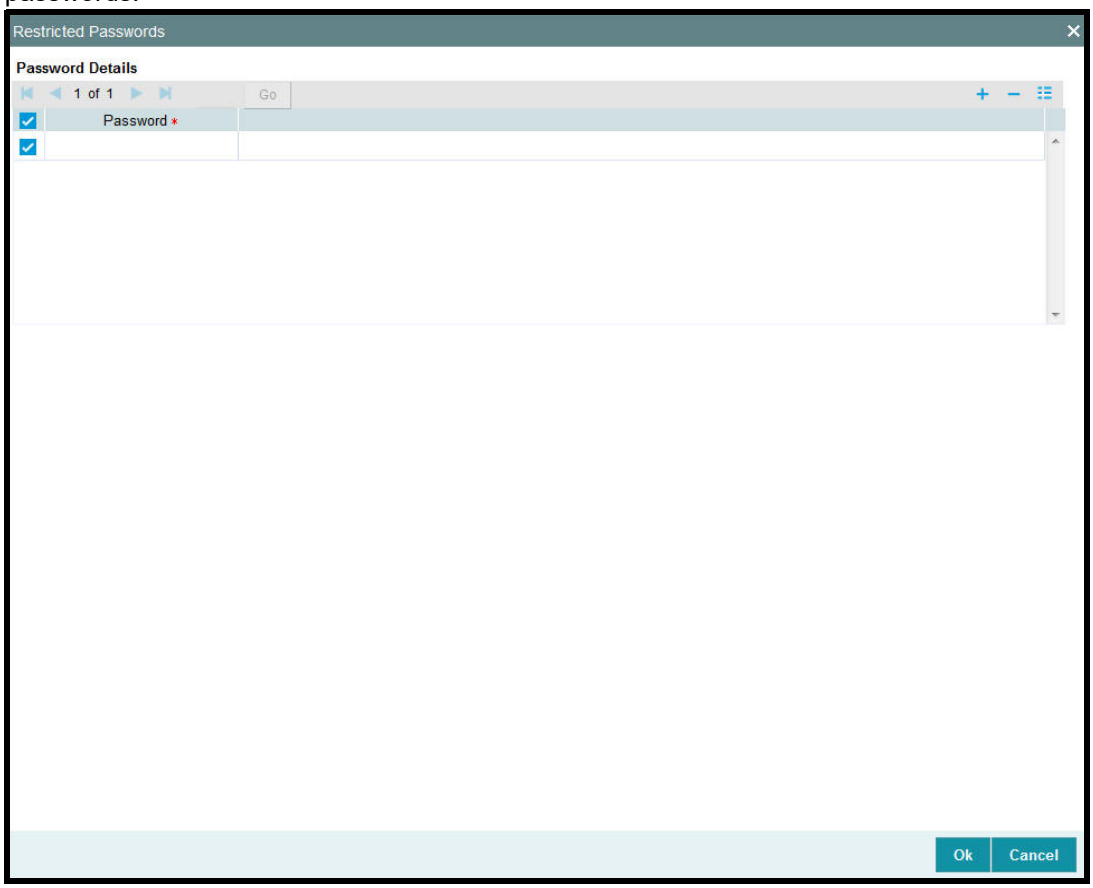
- XXX,XXX,XXX,XXX
- XX,XX,XX,XX,XXX

2.5.2 Restrictive Passwords Button

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.



Password Details

Password

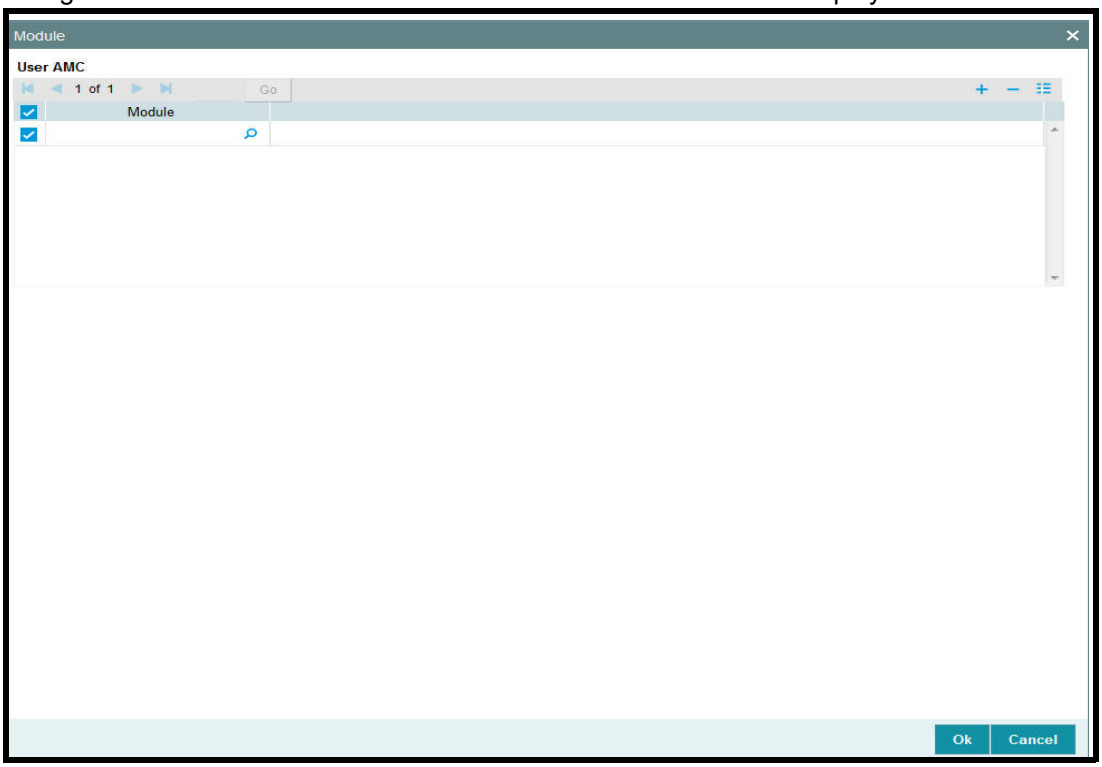
Alphanumeric; 12 Characters; Mandatory

Specify the restricted password.

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

2.5.3 Modules Button

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.



User AMC

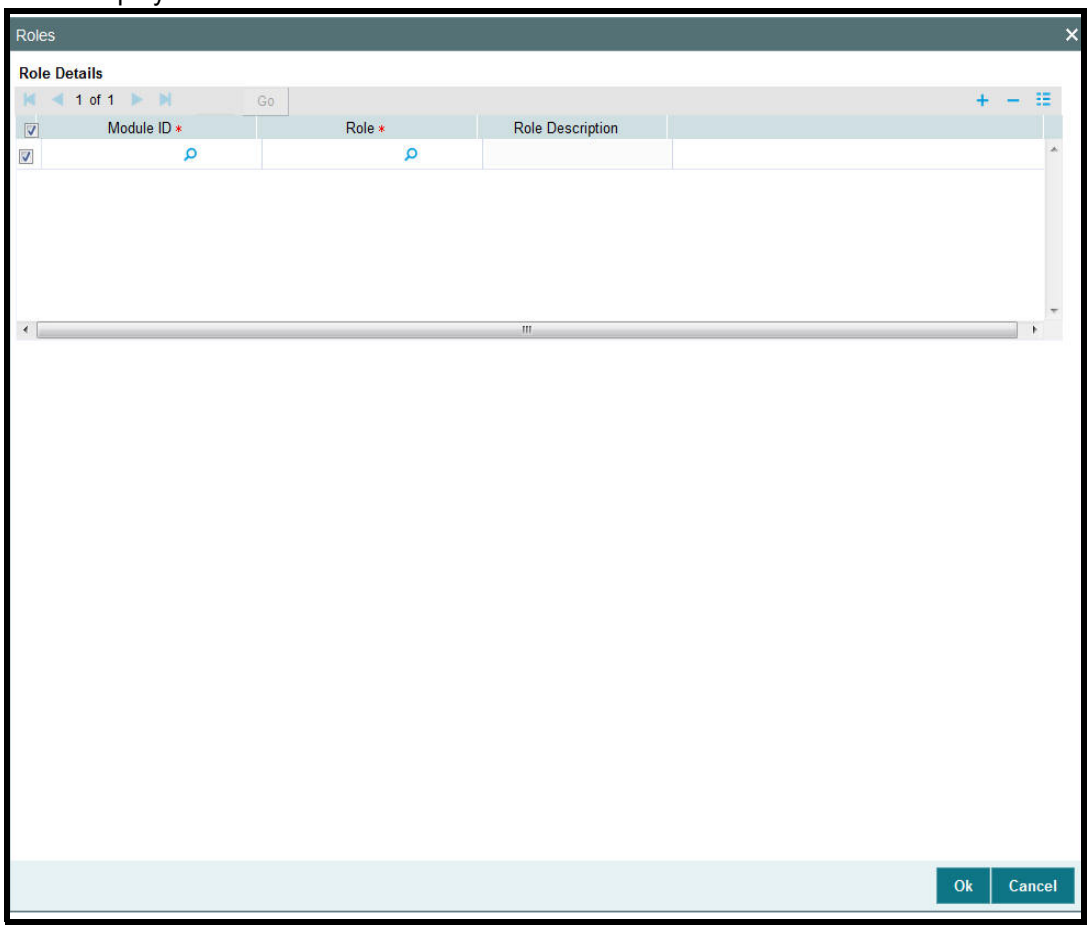
Module

Alphanumeric; 30 Characters; Optional

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

2.5.4 Roles Button

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



You can specify the following details:

Module ID

Alphanumeric; 30 Characters; Mandatory

Specify the module ID. Alternatively, you can select module ID code from the option list. The list displays all valid module ID maintained in the system.

Role

Alphanumeric; 15 Characters; Mandatory

Specify the role defined to the user.

Role Description

Display

The system displays the description for the selected 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.

2.5.5 Functions Button

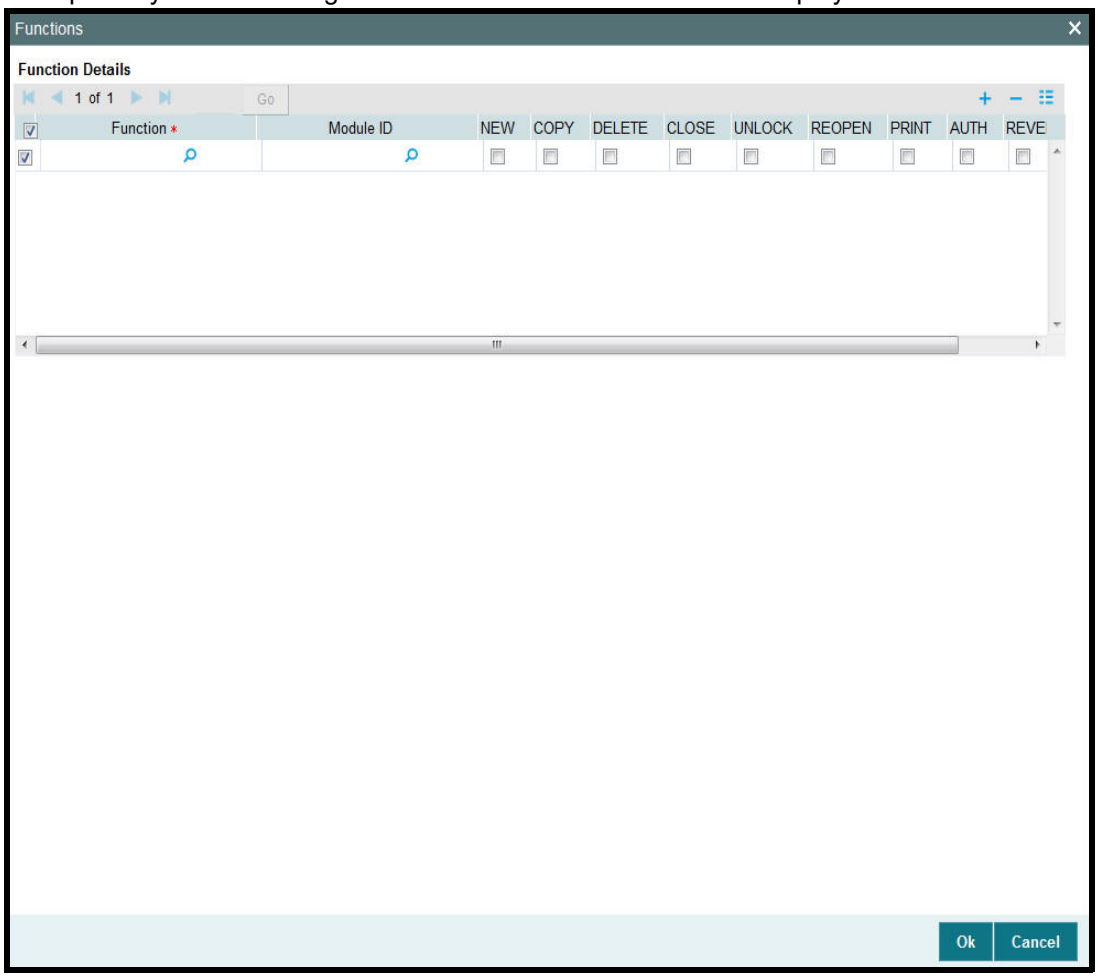
In addition to attaching a user profile to a role, you can give rights to individual functions. For a user profile to which no role is attached, you can give access to specific functions. If you have one of the following:

- 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.



Function

Alphanumeric; 3 Characters; Mandatory

Specify the branch code from the option list.

Module ID

Alphanumeric; 30 Characters; Mandatory

Specify the module ID from the option list.

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

2.5.5.1 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)
- Reverse (Reverse an existing record)

2.5.5.2 Contracts and On-line Transaction Processing

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

2.5.5.3 Reports

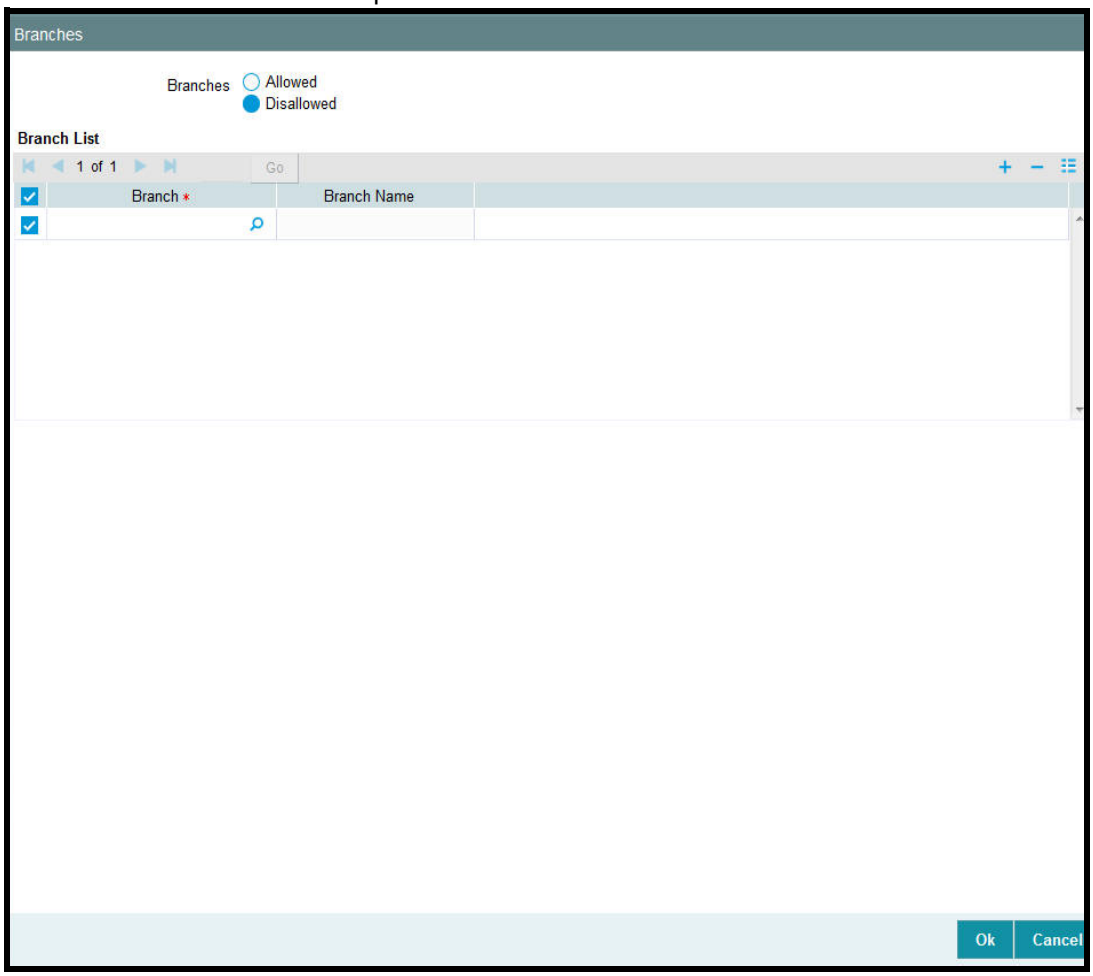
- Generate (to generate reports).
- View (view the reports).
- Print (print the reports).

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.

2.5.6 Branches Button

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.



Branches

Optional

Select one of the options from the following list:

- Allowed
- Disallowed

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.

Branch List

Branch

Alphanumeric; 3 Characters; Optional

Specify the branch code.

Branch Name

Display

The system displays the name of the branch for the selected branch code.

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.

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.

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.

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).

User Belonging to Customer Category

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

2.5.6.1 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.

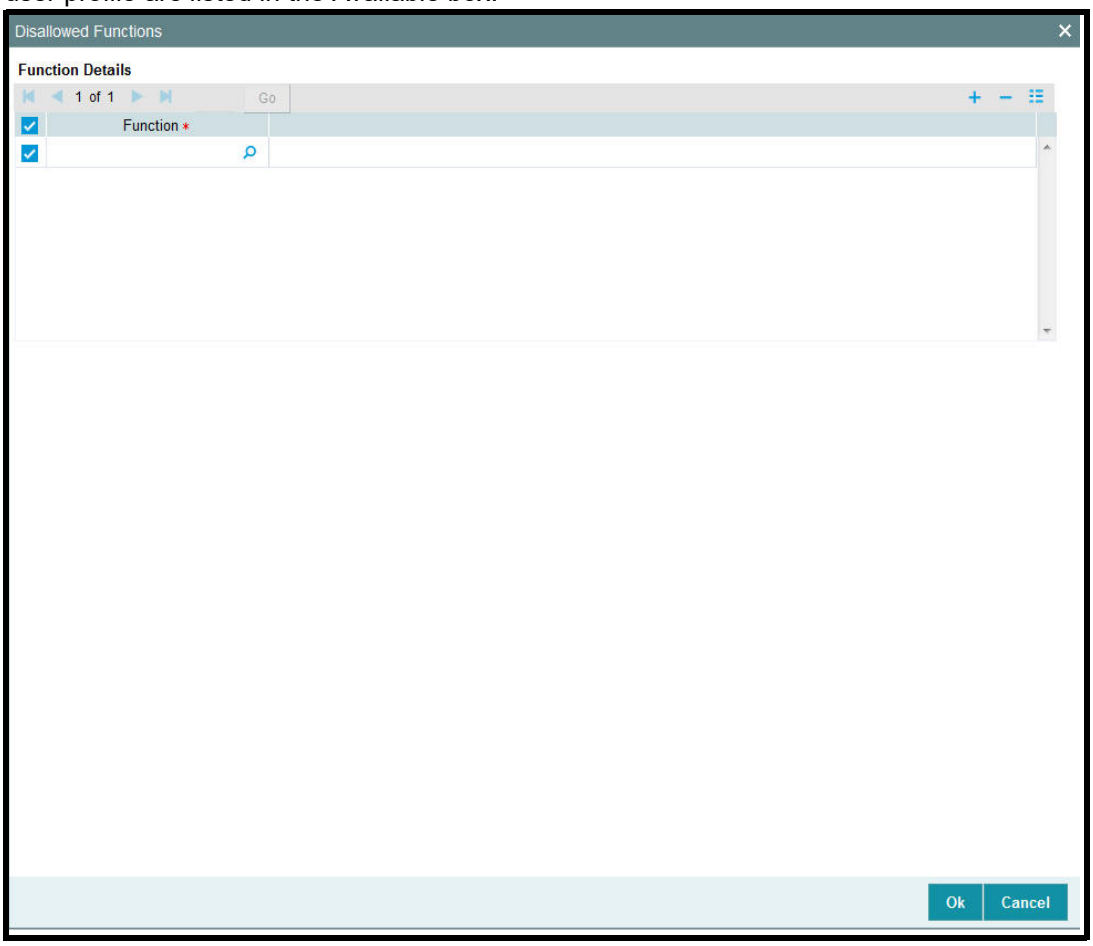
This validation is applicable only for UT transactions, Bulk transaction, adjustment transaction, light weight transaction and LEP – initial investment, top up, surrender and switch transaction types.

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.

2.5.7 Disallowed Functions Button

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.



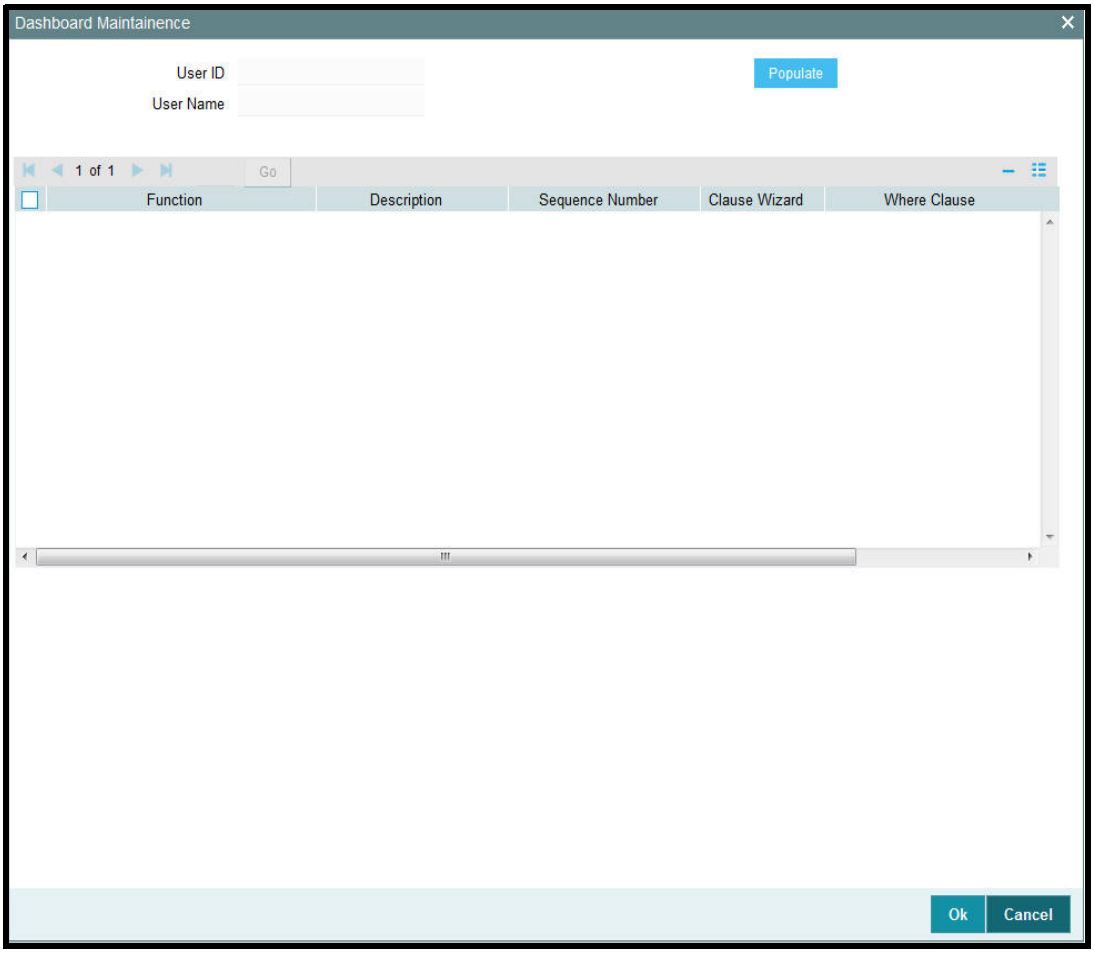
Function

Alphanumeric; 8 Characters; Mandatory

Select the functions that you wish to disallow for the user.

2.5.8 Dashboard Maintenance Button

Click ‘Dashboard Maintenance’ button in ‘User Admin’ screen to map the dashboards. The ‘Dashboard Maintenance’ screen is invoked.



User ID

Display

The system displays the user ID.

User Name

Display

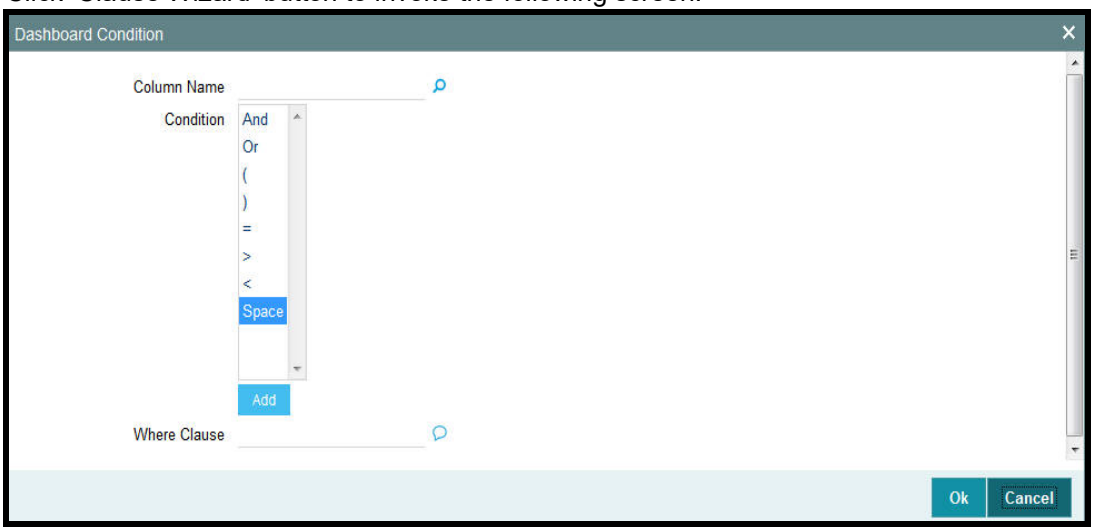
The system displays the user name for the selected user ID.

Click ‘Populate’ button, to view the following details:

- Function
- Description
- Sequence Number

Clause Wizard

Click ‘Clause Wizard’ button to invoke the following screen:



You can specify the following details:

Column Name

Alphanumeric; 35 Characters; Optional

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

Condition

Optional

Select the conditions from the drop-down list.

Where Clause

Alphanumeric; 35 Characters; Optional

Specify the where clause.

Show In Dashboard

Optional

Check this box to show in dashboard.

The system will default the value based on the value set at ‘User settings’ screen. If you uncheck this box, then the value will be applied upon change in modules.

2.5.9 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:

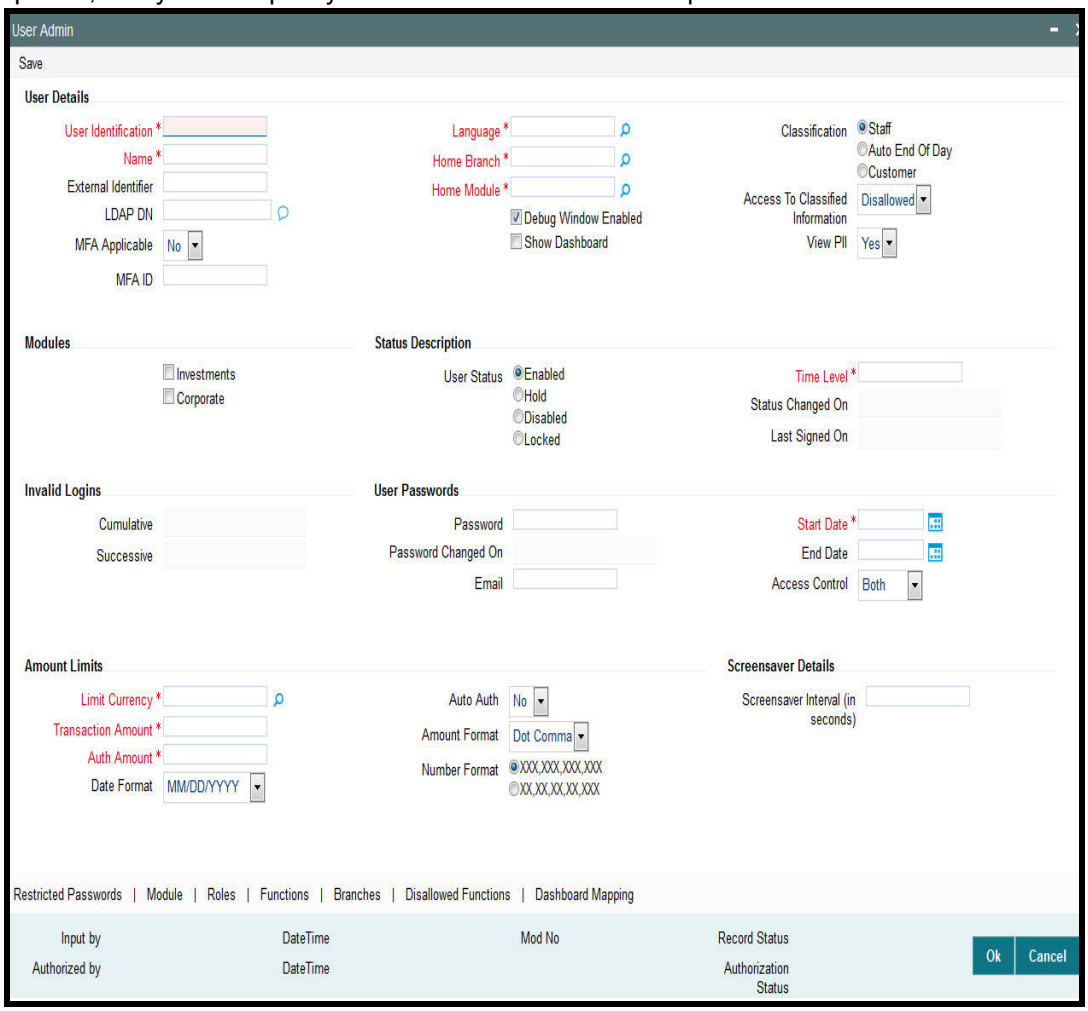
- The Rights button to define grant rights and grant queues for the user profile
- The User Till Restrictions button to define till restrictions for the user profile.
- The User Account Class Restrictions button to define a restrictive list of account classes for the user profile.
- The User GL Restrictions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

2.5.10 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.

2.5.11 Deleting User Profile

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

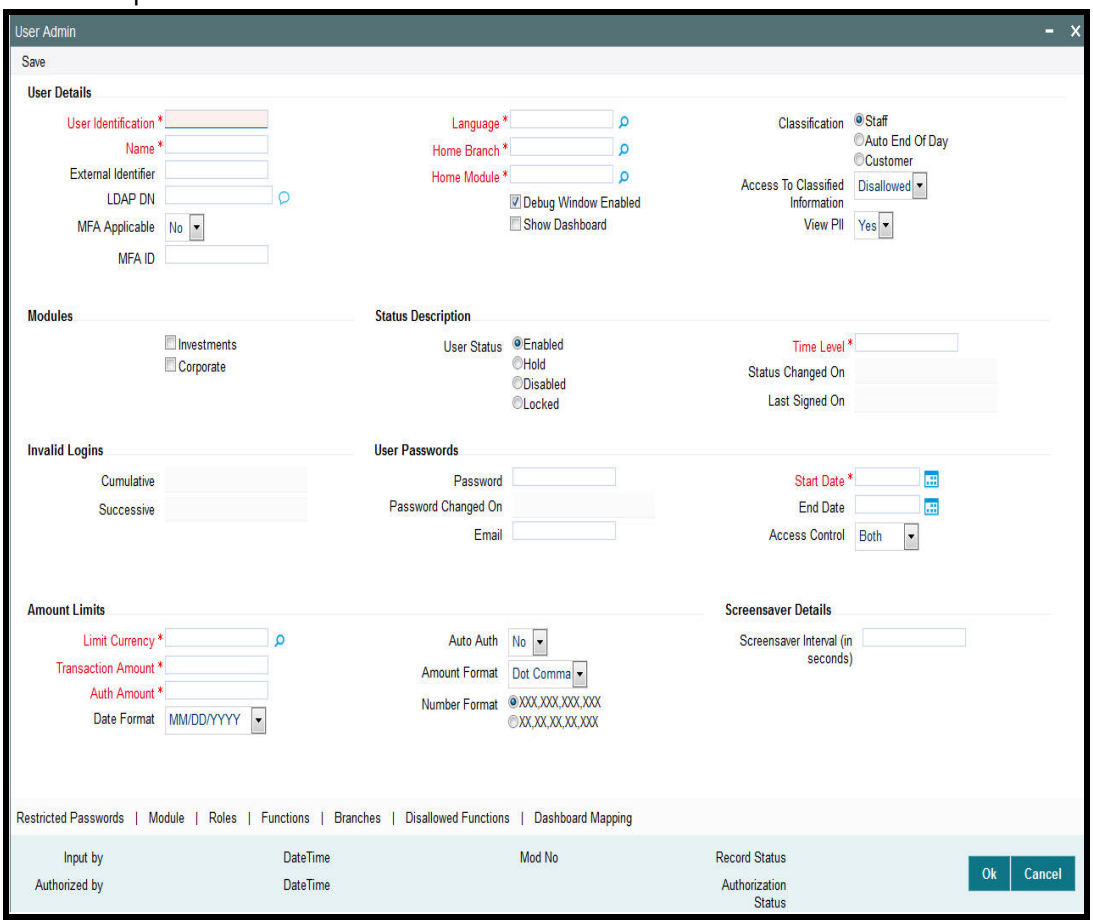
To delete an existing user profile, retrieve the record of the user profile so that it is displayed in the main portion of the User Profile Definition screen. Then select the Delete button from

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.

2.5.12 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.

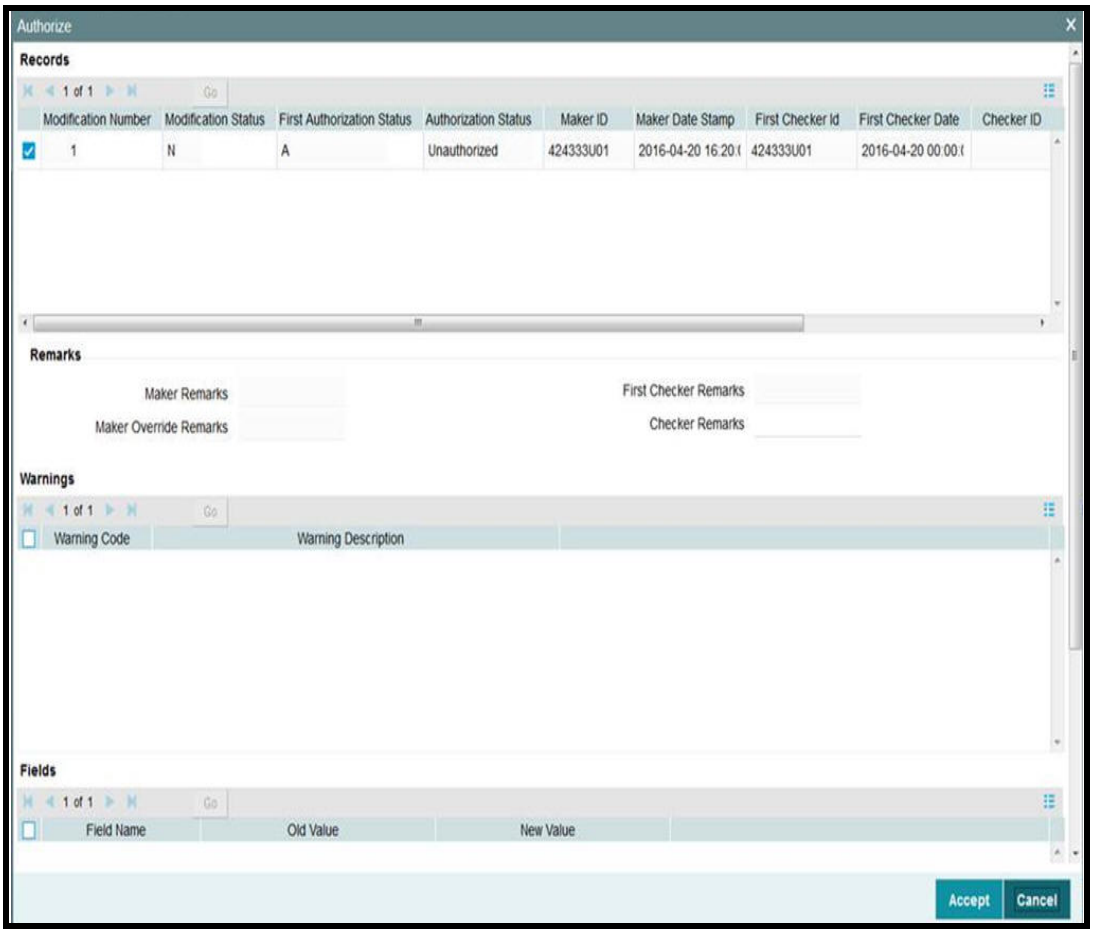
2.5.13 Authorizing User Profile

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.



2.5.14 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

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 Authorized field.
- The open status of the record, in the Open field.

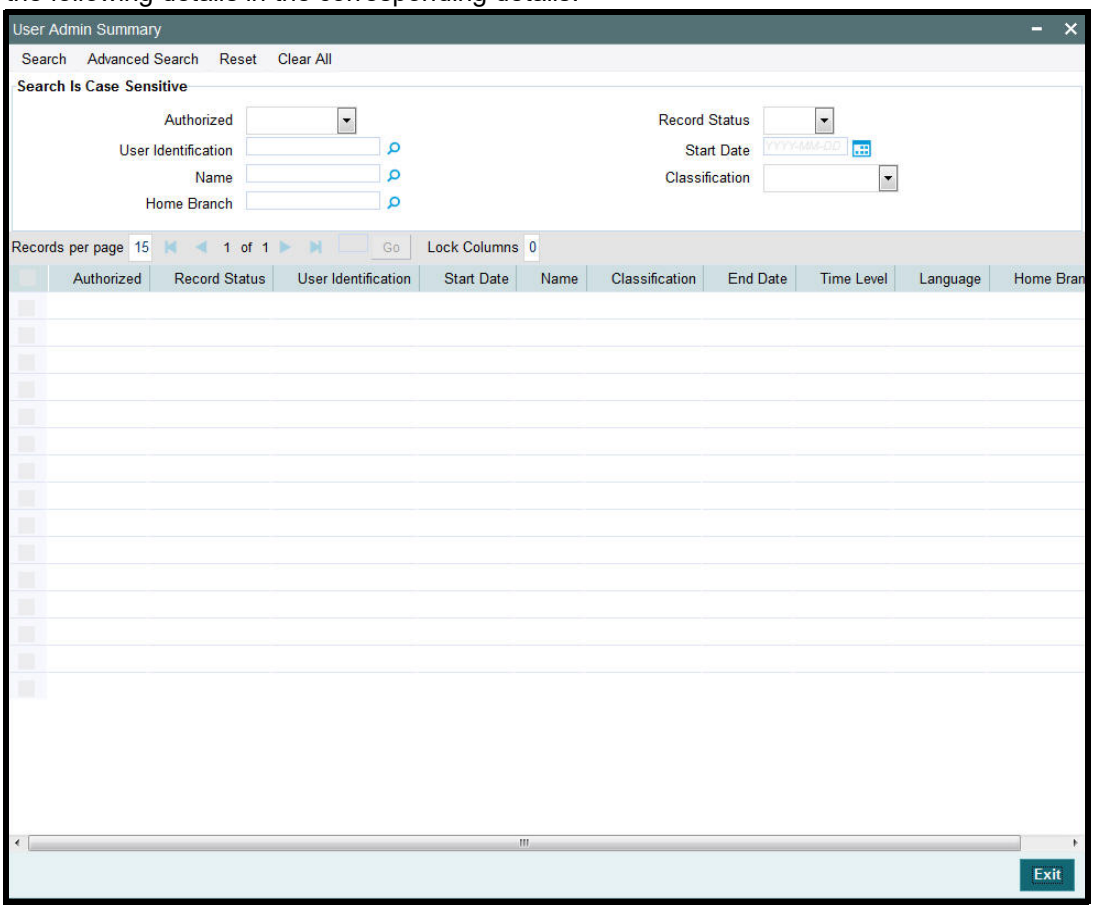
2.6 User Admin Summary

This section contains the following topics:

2.6.1 Retrieving a Record in User Admin Summary Screen

You can retrieve a previously entered record in the Summary Screen, as follows:

Invoke the ‘User Admin Summary’ screen by typing ‘SMSUSRDF’ in the field at the top right corner of the Application tool bar. Click on the adjoining arrow button and specify any or all of the following details in the corresponding details.



- The status of the record in the Authorized field. If you choose the ‘Blank Space’ option, then all the records are retrieved.
- The status of the record in the Record Status field. If you choose the ‘Blank Space’ option, then all records are retrieved
- User Identification
- Name
- Home Branch
- Start Date
- Classification

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

Note

You can also retrieve the individual record detail from the detail screen by querying in the following manner:

- Press F7
- Input the User Identification
- Press F8

You can perform Edit, Delete, Amend, Authorize, Reverse, Confirm operations by selecting the operation from the Action list. You can also search a record by using a combination of % and alphanumeric value

2.6.2 Editing User Admin Record

You can modify the details of User Admin record that you have already entered into the system, provided it has not subsequently authorized. You can perform this operation as follows:

- Invoke the User Admin Summary screen from the Browser.
- Select the status of the record that you want to retrieve for modification in the Authorization Status field. You can only modify records that are unauthorized. Accordingly, choose the Unauthorized option.
- Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.
- Click 'Search' button. All unauthorized 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 in the list of displayed records. The User Admin Maintenance screen is displayed.
- Select Unlock Operation from the Action list to modify the record. Modify the necessary information.

Click Save to save your changes. The User Admin screen is closed and the changes made are reflected in the User Admin Summary screen.

2.6.3 Viewing User Admin Record

To view a record that you have previously input, you must retrieve the same in the User Admin Summary screen as follows:

- Invoke the User Admin Summary screen from the Browser.
- Select the status of the record that you want to retrieve for viewing in the Authorization Status field. You can also view all records that are either unauthorized or authorized only, by choosing the unauthorized / Authorized option.
- Specify any or all of the details of the record in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to view in the list of displayed records. The User Admin screen is displayed in View mode.

2.6.4 Deleting User Admin Record

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

- Invoke the User Admin 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 in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to delete in the list of displayed records. The User Admin screen is displayed.

- Select Delete Operation from the Action list. The system prompts you to confirm the deletion and the record is physically deleted from the system database.

2.6.5 Authorizing User Admin Record

- An unauthorized User Admin record must be authorized in the system for it to be processed. To authorize a record:
- Invoke the User Admin Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. Typically, choose the unauthorized option.
- Specify any or all of the details in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.
- Double click the record that you wish to authorize. The User Admin screen is displayed. Select Authorize operation from the Action List.

When a checker authorizes a record, details of validation, if any, that were overridden by the maker of the record during the Save operation are displayed. If any of these overrides results in an error, the checker must reject the record.

2.6.6 Amending User Admin Record

After a User Admin record is authorized, it can be modified using the Unlock operation from the Action List. To make changes to a record after authorization:

- Invoke the User Admin Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. You can only amend authorized records.
- Specify any or all of the details in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.
- Double click the record that you wish to authorize. The User Admin screen is displayed in amendment mode. Select Unlock operation from the Action List to amend the record.
- Amend the necessary information and click on Save to save the changes

2.6.7 Authorizing Amended User Admin Record

An amended User Admin record must be authorized for the amendment to be made effective in the system. The authorization of amended records can be done only from Fund Manager Module and Agency Branch module.

The subsequent process of authorization is the same as that for normal transactions.

2.7 Hot Key Maintenance

This section contains the following topics:

2.7.1 Maintaining Hot Keys

You can set the most used screens in hot keys and launch the same using the hot key combination. By using the hot keys, you can avoid typing function IDs or using the menu path.

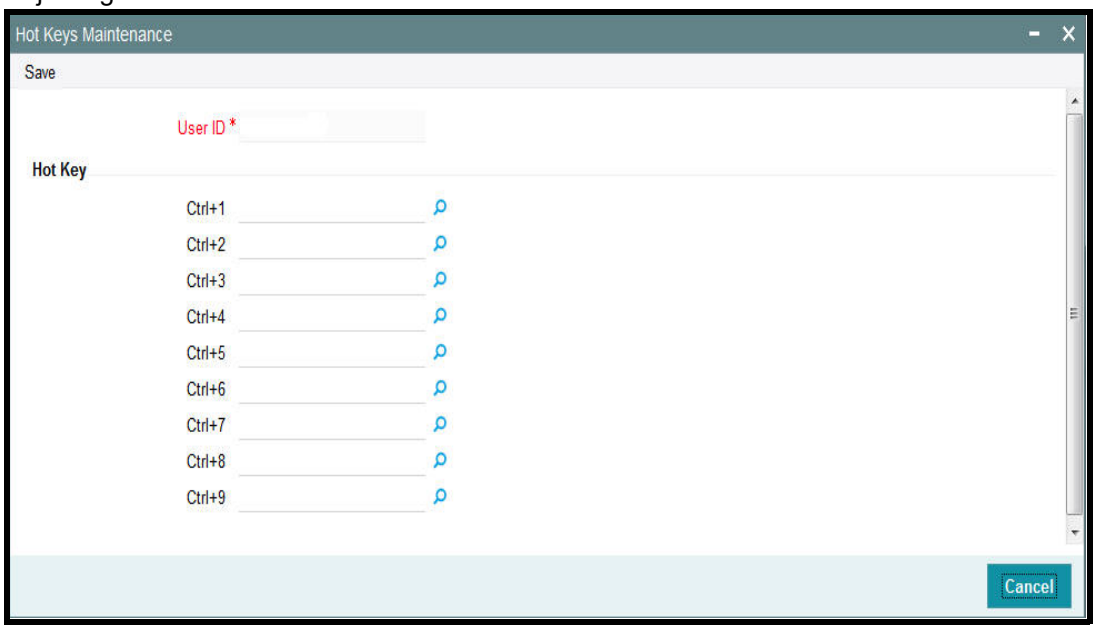
You can use hot keys with the key combinations from Ctrl+1 to Ctrl+9. In the predefined key combination, you can save the required function IDs. Based on the role/ function mapped the function ID will be listed in the screen.

When you click any of the function ID saved for particular key stroke from fast track the corresponding screen will be launched.

Note

Maximum number of Hot keys that can be entered is 9. Same key combination cannot be used for different function id in different modules.

You can invoke 'Hot Keys Maintenance' screen by typing 'SMDHOTKY/ UTDHOTKY' based on the module in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button.



You can specify the following details:

User ID

Display

The system displays the logged in user ID.

Hot Key

Ctr+1

Alphanumeric; 8 Characters; Optional

Specify the valid function ID for the logged in user. Alternatively, you can select the valid function IDs from the option list. The list displays all valid function IDs maintained in the system.

Ctr+2

Alphanumeric; 8 Characters; Optional

Specify the valid function ID for the logged in user. Alternatively, you can select the valid function IDs from the option list. The list displays all valid function IDs maintained in the system.

Ctr+3

Alphanumeric; 8 Characters; Optional

Specify the valid function ID for the logged in user. Alternatively, you can select the valid function IDs from the option list. The list displays all valid function IDs maintained in the system.

Ctr+4

Alphanumeric; 8 Characters; Optional

Specify the valid function ID for the logged in user. Alternatively, you can select the valid function IDs from the option list. The list displays all valid function IDs maintained in the system.

Ctr+5

Alphanumeric; 8 Characters; Optional

Specify the valid function ID for the logged in user. Alternatively, you can select the valid function IDs from the option list. The list displays all valid function IDs maintained in the system.

Ctr+6

Alphanumeric; 8 Characters; Optional

Specify the valid function ID for the logged in user. Alternatively, you can select the valid function IDs from the option list. The list displays all valid function IDs maintained in the system.

Ctr+7

Alphanumeric; 8 Characters; Optional

Specify the valid function ID for the logged in user. Alternatively, you can select the valid function IDs from the option list. The list displays all valid function IDs maintained in the system.

Ctr+8

Alphanumeric; 8 Characters; Optional

Specify the valid function ID for the logged in user. Alternatively, you can select the valid function IDs from the option list. The list displays all valid function IDs maintained in the system.

Ctr+9

Alphanumeric; 8 Characters; Optional

Specify the valid function ID for the logged in user. Alternatively, you can select the valid function IDs from the option list. The list displays all valid function IDs maintained in the system.

2.8 Clearing Users

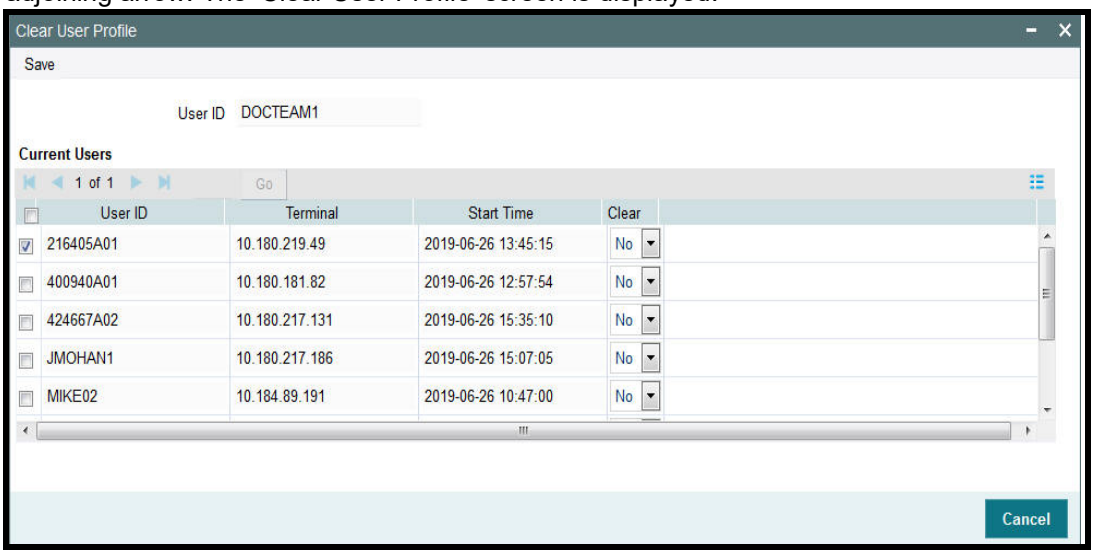
This section contains the following topics:

- Section 2.8.1, "Clearing User that has Exited System Abnormally"

2.8.1 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/ UTDCLUSR’ 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.



User ID

Display

The system displays the user ID.

Current Users

The system displays the following values:

- User ID
- Terminal
- Start Time

Clear

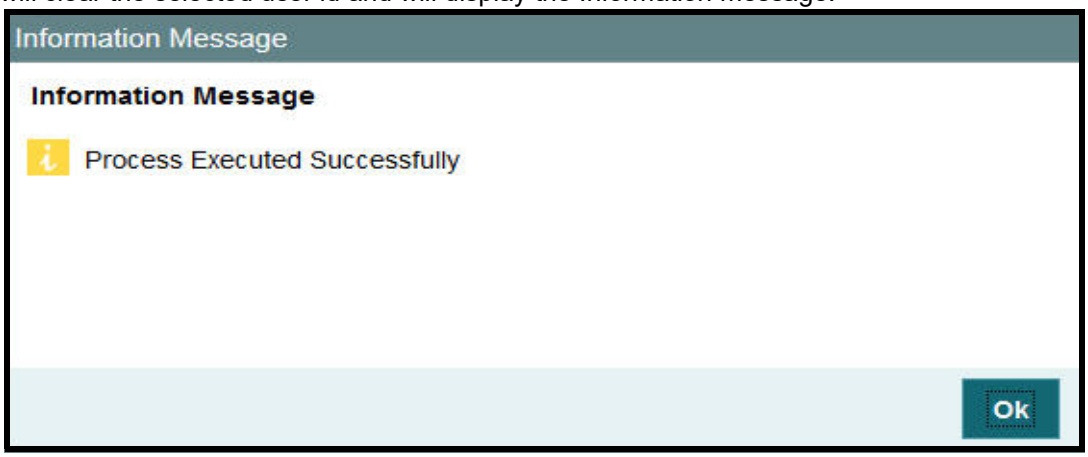
Optional

Select if the specified user has to be cleared or not from he drop-down list. The list displays the following values:

- Yes
- No

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 User ID, terminal and start time information. Select the option ‘Yes’ from ‘Clear’ drop-down to clear the selected user.

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 Information message:



Click on OK to confirm.

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

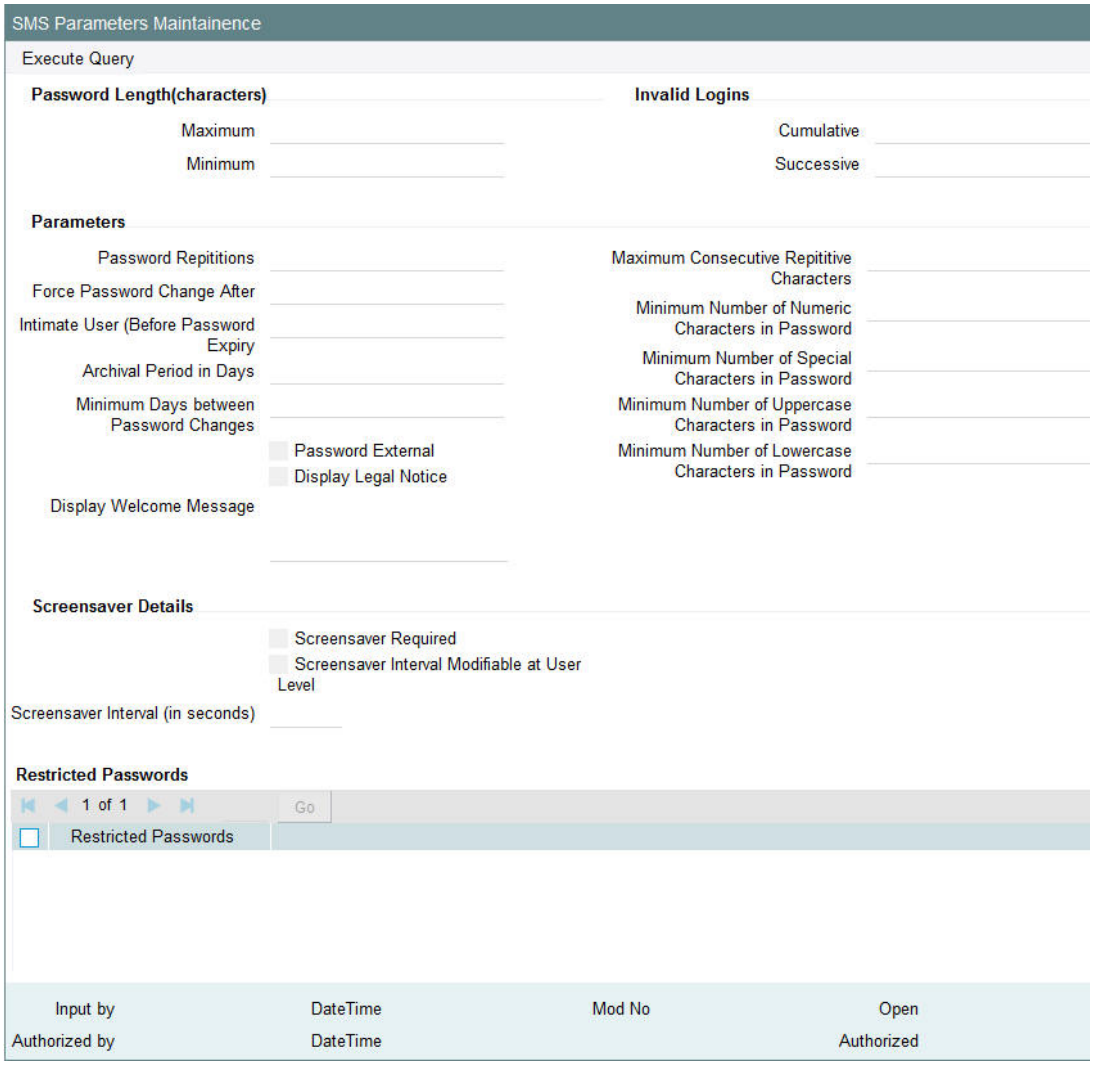
2.9 SMS Parameters

This section contains the following topics:

- Section 2.9.1, "Setting up SMS Parameters"

2.9.1 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.



Click ‘Enter Query’ to display the SMS parameters. However, you can amend the values by clicking ‘Unlock’ option.

Password Length (Characters)

Maximum

Numeric; 2 Characters; 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; 2 Characters; 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.

Invalid Logins

Cumulative

Numeric; 2 Characters; 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; 1 Character; 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.

Parameters

Password Repetitions

Numeric; 1 Character; 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; 3 Characters; 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.

Intimate User (Before Password Expiry)

Numeric, 1 Character; 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.

Archival Period in Days

Numeric; 3 Characters; Optional

Specify the archival period.

Minimum Days between Password Changes

Numeric; 3 Characters; 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.

Password External

Optional

Check this box if the password is external.

Display Legal Notice

Optional

Check this box to display the legal notice.

Display Welcome Message

Alphanumeric; 4000 Characters; Optional

Specify the welcome text message to be displayed on launching the login screen,

Maximum Consecutive Repetitive Characters

Numeric; 2 Characters; 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; 2 Characters; 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; 2 Characters; 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 Uppercase Characters in Password

Numeric; 2 Characters; Optional

You can define the minimum number of uppercase characters allowed in a user password. The allowed uppercase 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 Uppercase Characters = 1
- Maximum No of Numeric Characters = Maximum Password Length

Minimum Number of Lowercase Characters in Password

Numeric; 2 Characters; Optional

You can define the minimum number of lowercase characters allowed in a user password. The allowed lowercase 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 Lowercase Characters = 1
- Maximum No of Numeric Characters = Maximum Password Length

Screensaver Details

Screensaver Required

Optional

Check this box if screensaver is required.

Screensaver Interval Modifiable at User Level

Optional

Check this box if screensaver interval can be modified at user level.

Screensaver Interval (in seconds)

Numeric; 4 Characters; Optional

Specify the screen saver interval.

Restricted Passwords

Restricted Passwords

Alphanumeric; 12 Characters; Optional

Specify the restricted password.

2.10 User Details Modification in Bulk

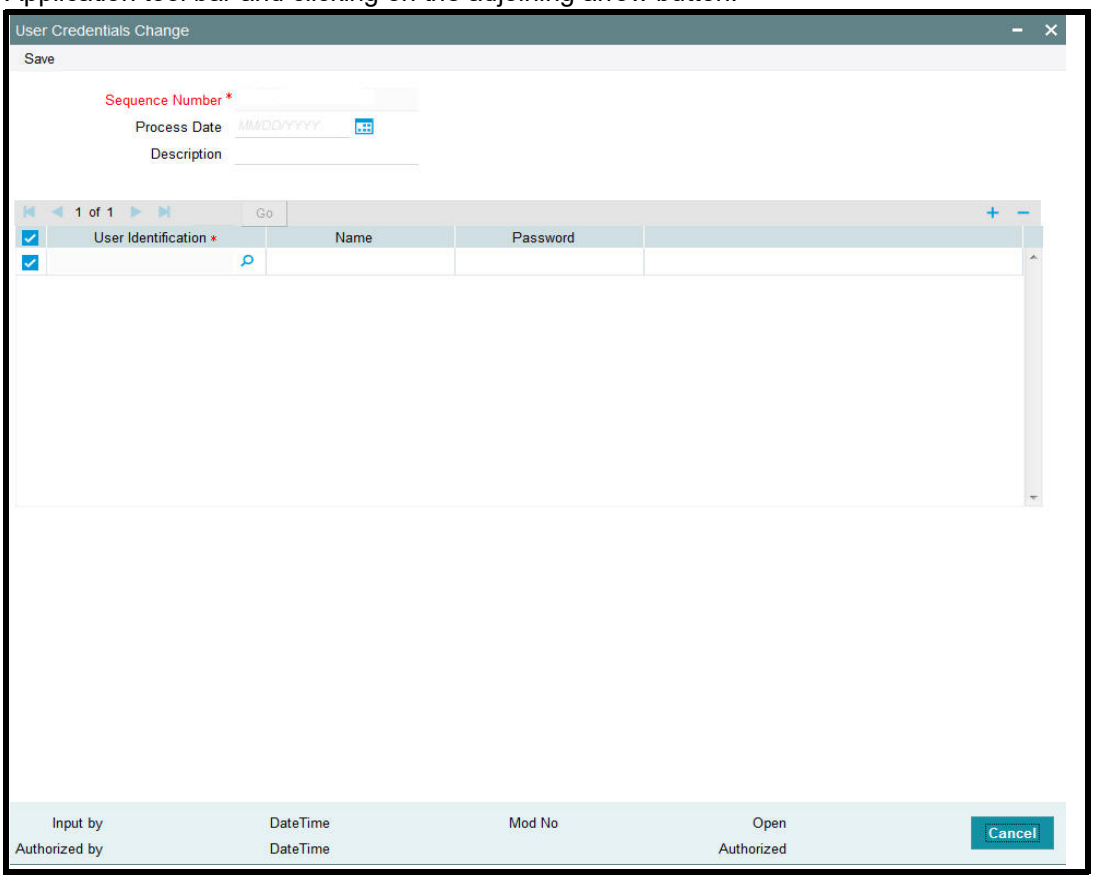
This section contains the following topics:

- Section 2.10.1, "Modifying User Details in Bulk"

2.10.1 Modifying User Details 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

Display

Click on ‘New’ icon to generate a new ‘Sequence Number’.

Process Date

Date Format; Optional

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

Description

Alphanumeric, 35 Characters; Optional

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

User Identification

Alphanumeric, 12 Characters; Mandatory

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

Name

Display

The system displays the name of the user specific to the selected user ID.

Password

Alphanumeric; 32 Characters; 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.

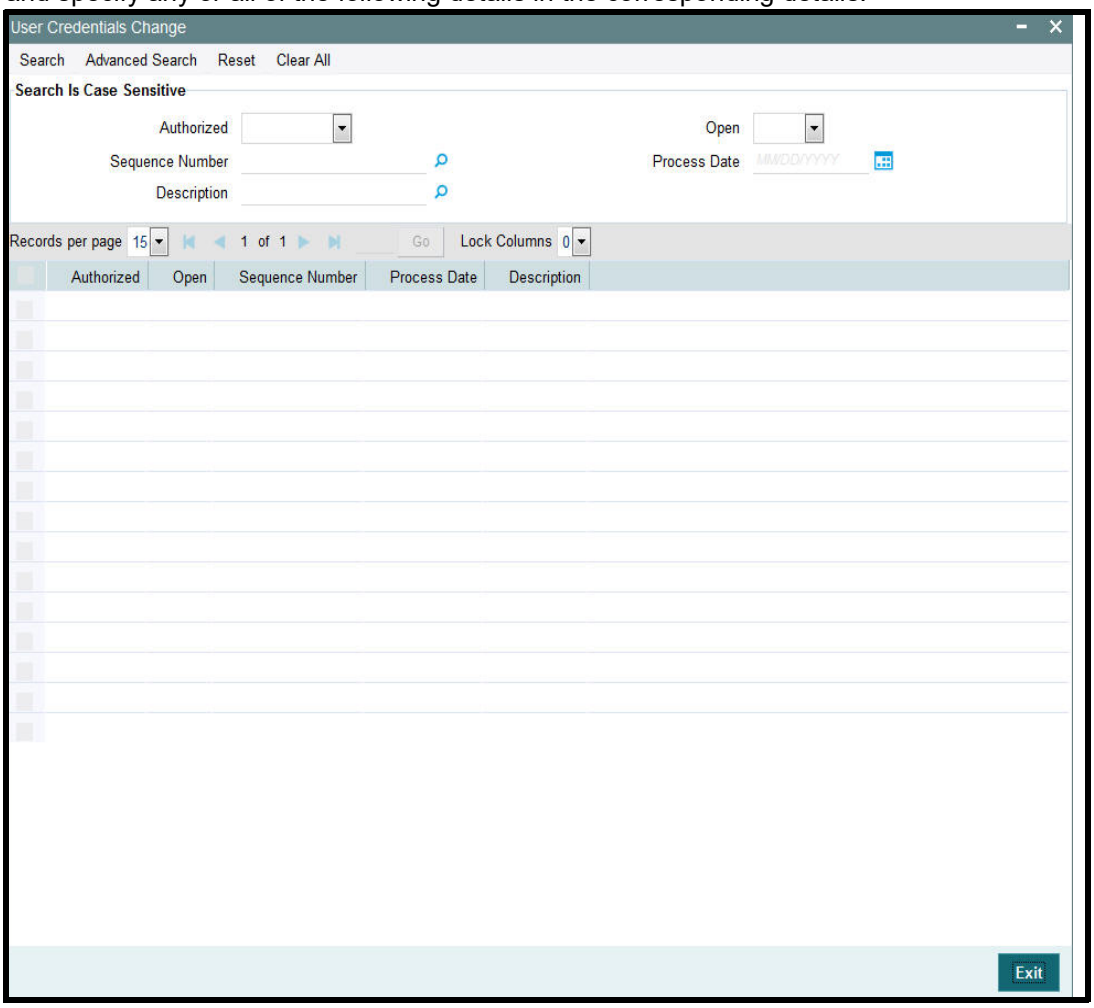
2.11 User Credentials Change Summary

This section contains the following topics:

2.11.1 Retrieving a Record in User Credentials Change Summary Screen

You can retrieve a previously entered record in the Summary screen, as follows:

Invoke the ‘User Credentials Change Summary’ screen by typing ‘SMSCHPWD’ in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button and specify any or all of the following details in the corresponding details.



- The status of the record in the Authorization Status field. If you choose the ‘Blank Space’ option, then all the records are retrieved.
- The status of the record in the Open field. If you choose the ‘Blank Space’ option, then all records are retrieved
- Sequence Number
- Description
- Process Date

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

Note

You can also retrieve the individual record detail from the detail screen by querying in the following manner:

- Press F7
- Input the Sequence Number
- Press F8

You can perform Edit, Delete, Amend, Authorize, operations by selecting the operation from the Action list. You can also search a record by using a combination of % and alphanumeric value

2.11.2 Editing User Credentials Change Record

You can modify the details of User Credentials Change record that you have already entered into the system, provided it has not subsequently authorized. You can perform this operation as follows:

- Invoke the User Credentials Change Summary screen from the Browser.
- Select the status of the record that you want to retrieve for modification in the Authorization Status field. You can only modify records that are unauthorized. Accordingly, choose the Unauthorized option.
- Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.
- Click 'Search' button. All unauthorized 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 in the list of displayed records. The User Credentials Change Detail screen is displayed.
- Select Unlock Operation from the Action list to modify the record. Modify the necessary information.

Click Save to save your changes. The User Credentials Change Detail screen is closed and the changes made are reflected in the User Credentials Change Summary screen.

2.11.3 Viewing User Credentials Change Record

To view a record that you have previously input, you must retrieve the same in the User Credentials Change Summary screen as follows:

- Invoke the User Credentials Change Summary screen from the Browser.
- Select the status of the record that you want to retrieve for viewing in the Authorization Status field. You can also view all records that are either unauthorized or authorized only, by choosing the unauthorized / Authorized option.
- Specify any or all of the details of the record in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to view in the list of displayed records. The User Credentials Change Detail screen is displayed in View mode.

2.11.4 Deleting User Credentials Change Record

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

- Invoke the User Credentials Change 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 in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to delete in the list of displayed records. The User Credentials Change Detail screen is displayed.

- Select Delete Operation from the Action list. The system prompts you to confirm the deletion and the record is physically deleted from the system database.

2.11.5 Authorizing User Credentials Change Record

- An unauthorized User Credentials Change record must be authorized in the system for it to be processed. To authorize a record:
- Invoke the User Credentials Change Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. Typically, choose the unauthorized option.
- Specify any or all of the details in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.
- Double click the record that you wish to authorize. The User Credentials Change Detail screen is displayed. Select Authorize operation from the Action List.

When a checker authorizes a record, details of validation, if any, that were overridden by the maker of the record during the Save operation are displayed. If any of these overrides results in an error, the checker must reject the record.

2.11.6 Amending User Credentials Change Record

After a User Credentials Change record is authorized, it can be modified using the Unlock operation from the Action List. To make changes to a record after authorization:

- Invoke the User Credentials Change Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. You can only amend authorized records.
- Specify any or all of the details in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.
- Double click the record that you wish to authorize. The User Credentials Change Detail screen is displayed in amendment mode. Select Unlock operation from the Action List to amend the record.
- Amend the necessary information and click on Save to save the changes

2.11.7 Authorizing Amended User Credentials Change Record

An amended User Credentials Change record must be authorized for the amendment to be made effective in the system. The authorization of amended records can be done only from Fund Manager Module and Agency Branch module.

The subsequent process of authorization is the same as that for normal transactions.

2.12 Modules

This section contains the following topics:

2.12.1 Setting up 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.

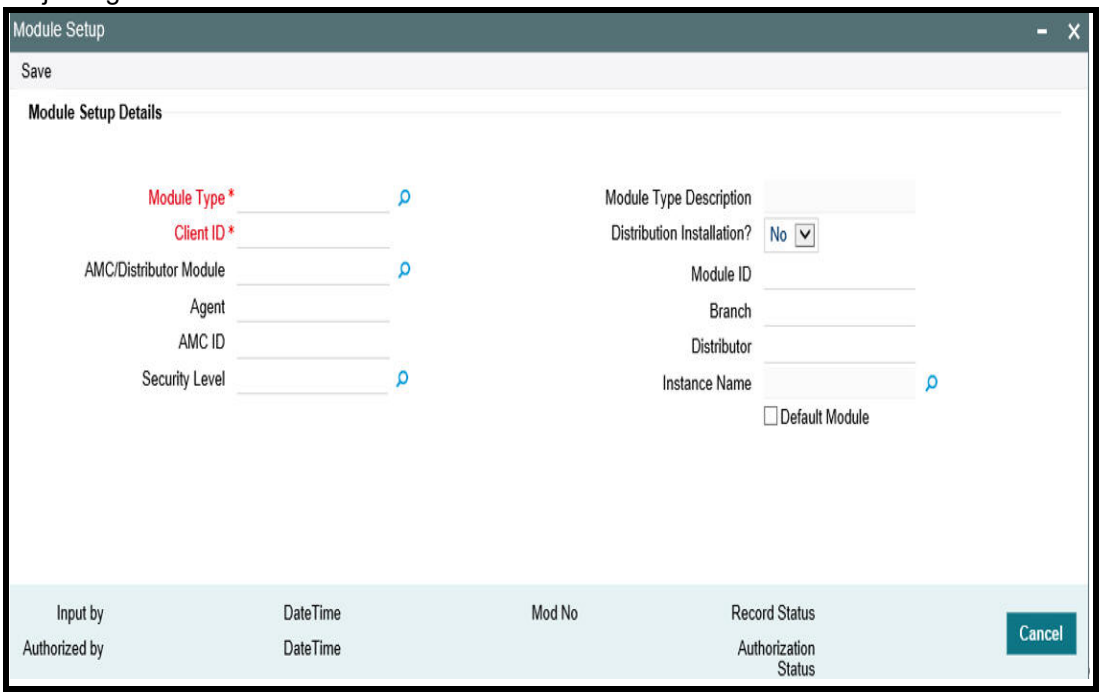
Each instance of the installation, in a multi-networked situation, is referred to a Module.

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

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 system admin User must set up the Agency Branch module.

Subsequently, if any new agency branch modules need to be created, the system admin 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.



To set up a module, specify the following details:

Module Type

Alphanumeric; 3 Characters; Mandatory

Specify the module type. Alternatively, you can select module type from the option list. The list displays all valid module types maintained in the system.

Module Type Description

Display

The system displays the description for the selected module type.

Distribution Installation?

Optional

Select if distribution installation is required or not from the drop-down list. The list displays the following values:

- Yes
- No

Client ID

Alphanumeric; 15 Characters; Mandatory

Specify the client ID for which the module is being created.

This field is enabled only if you have selected ‘Fund Manager’ or ‘Service Provider’ option in ‘Module Type’ field.

Module ID

Alphanumeric; 30 Characters; Optional

Specify the module ID.

This must be unique, and if any duplicates are detected by the system, a warning message is displayed.

The system displays the client ID for the selected module in case of Fund Manager or Service Provider.

This field is disabled if you have selected ‘Fund Manager’ or ‘Service Provider’ option in ‘Module Type’ field.

Branch

Alphanumeric; 12 Characters; Mandatory

Specify the branch code.

AMC/Distributor Module

Alphanumeric; 30 Characters; Optional

Specify AMC or distributor module.

This field will be display field if you have selected ‘Fund Manager’ or ‘Service Provider’ option in ‘Module Type’ field.

Distributor

Alphanumeric; 12 Characters; Mandatory

Specify the distributor details.

Agent

Alphanumeric; 12 Characters; Mandatory

Specify the agent code.

AMC ID

Alphanumeric; 12 Characters; Optional

Specify the AMC ID.

Instance Name

Alphanumeric; 50 Characters; Optional

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

Security Level

Alphanumeric; 2 Characters; Optional

Specify the security level.

Default Module

Optional

Select this option to set to default module.

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.

2.12.2 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:

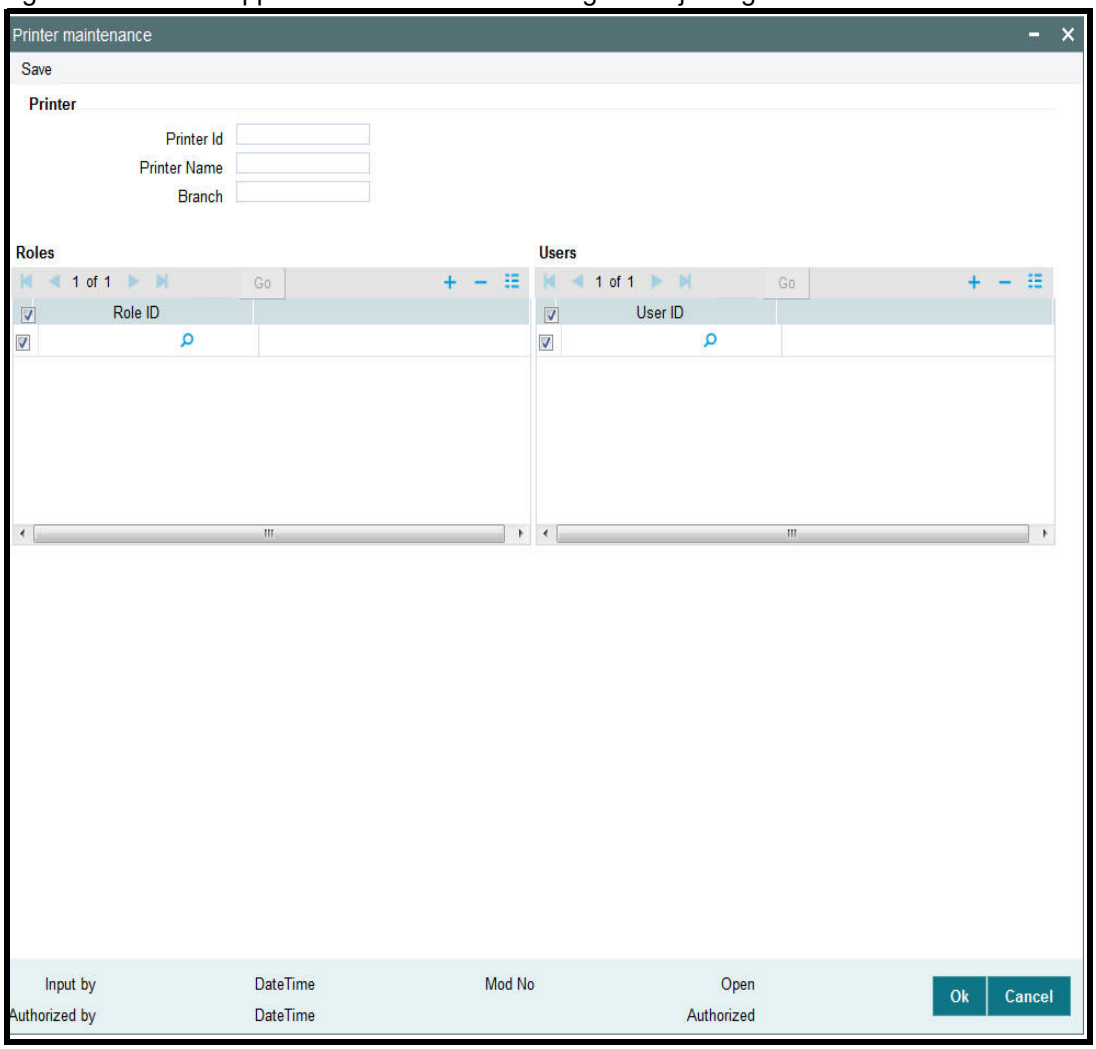
- Retrieval for viewing
- Editing unauthorized modules
- Deleting unauthorized modules
- Authorizing modules
- Amending authorized modules

2.13 Printer Maintenance

This section contains the following topics:

2.13.1 Invoking Printer Maintenance Detail Screen

You can invoke ‘Printer Maintenance’ screen by typing ‘SMDPRTMN’ 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:

Printer

Printer ID

Alphanumeric; 2 Characters; Optional

Specify the printer ID.

Printer Name

Alphanumeric; 105 Characters; Optional

Specify the printer name.

Branch

Alphanumeric; 3 Characters; Optional

Specify the branch code.

Roles

Role ID

Alphanumeric; 15 Characters; Optional

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

Users

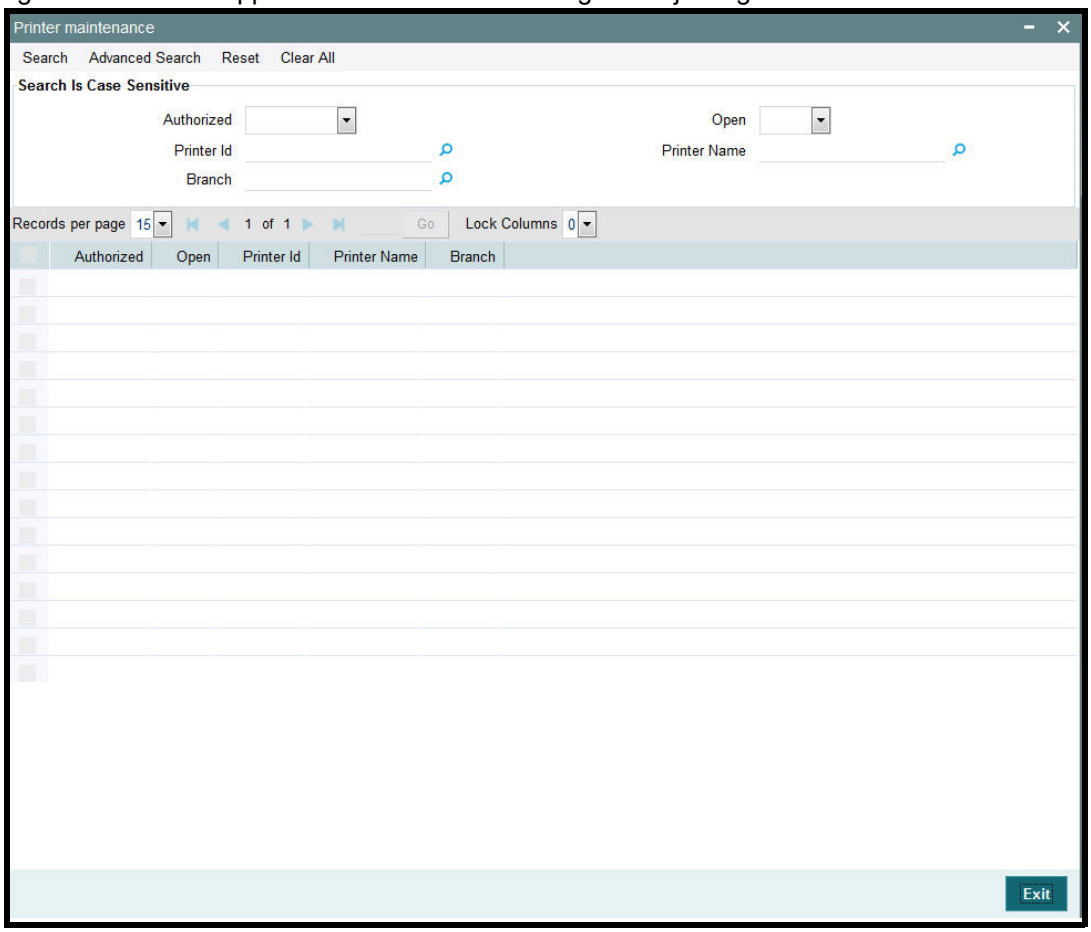
User ID

Alphanumeric; 12 Characters; Optional

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

2.13.2 Invoking Printer Maintenance Screen

You can invoke ‘Printer Maintenance’ screen by typing ‘SMSPRTMN’ in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.



You can retrieve a previously entered record in the ‘Printer Maintenance’ screen, as follows:. Specify any or all of the following details in the ‘Printer Maintenance’ screen:

- The status of the record to be printed in the Authorized field. If you choose the “Blank Space” option, then all the records to be printed are retrieved.
- The status of the record in the Open field. If you choose the “Blank Space” option, then all the records to be printed are retrieved.

- Printer ID
- Printer Name
- Branch

Click save icon to save your record. The system confirms the saving of the record.

2.13.3 Operations on Printing a Record

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

Before the record 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 Printer Maintenance screen can be used for the following operations on records:

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

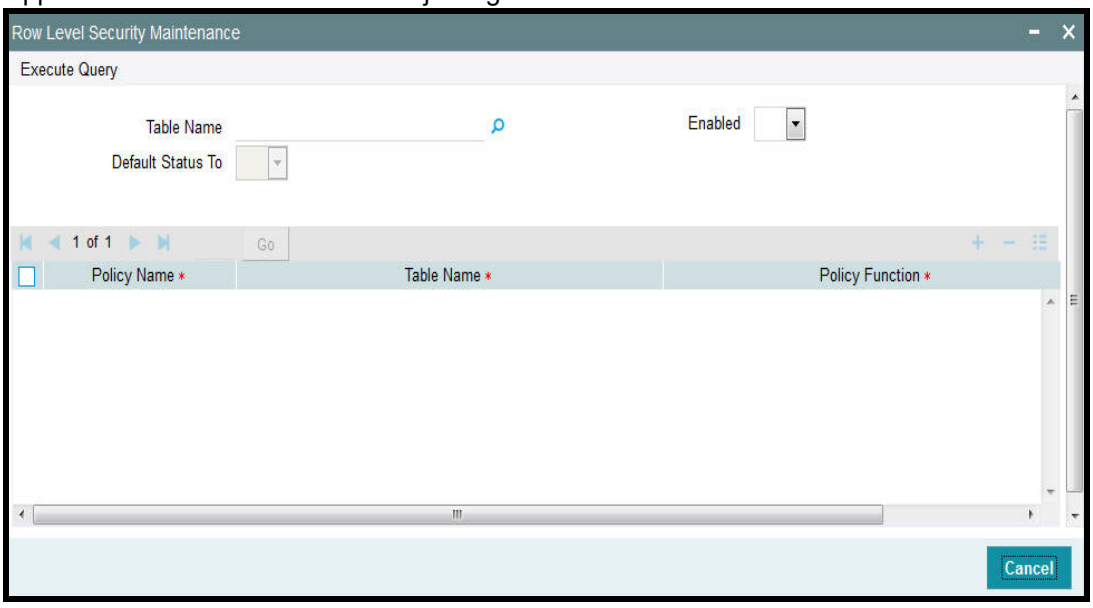
2.14 Row Level Security Maintenance

This section contains the following topics:

- Section 2.14.1, "Invoking Row Level Security Maintenance Screen"

2.14.1 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.

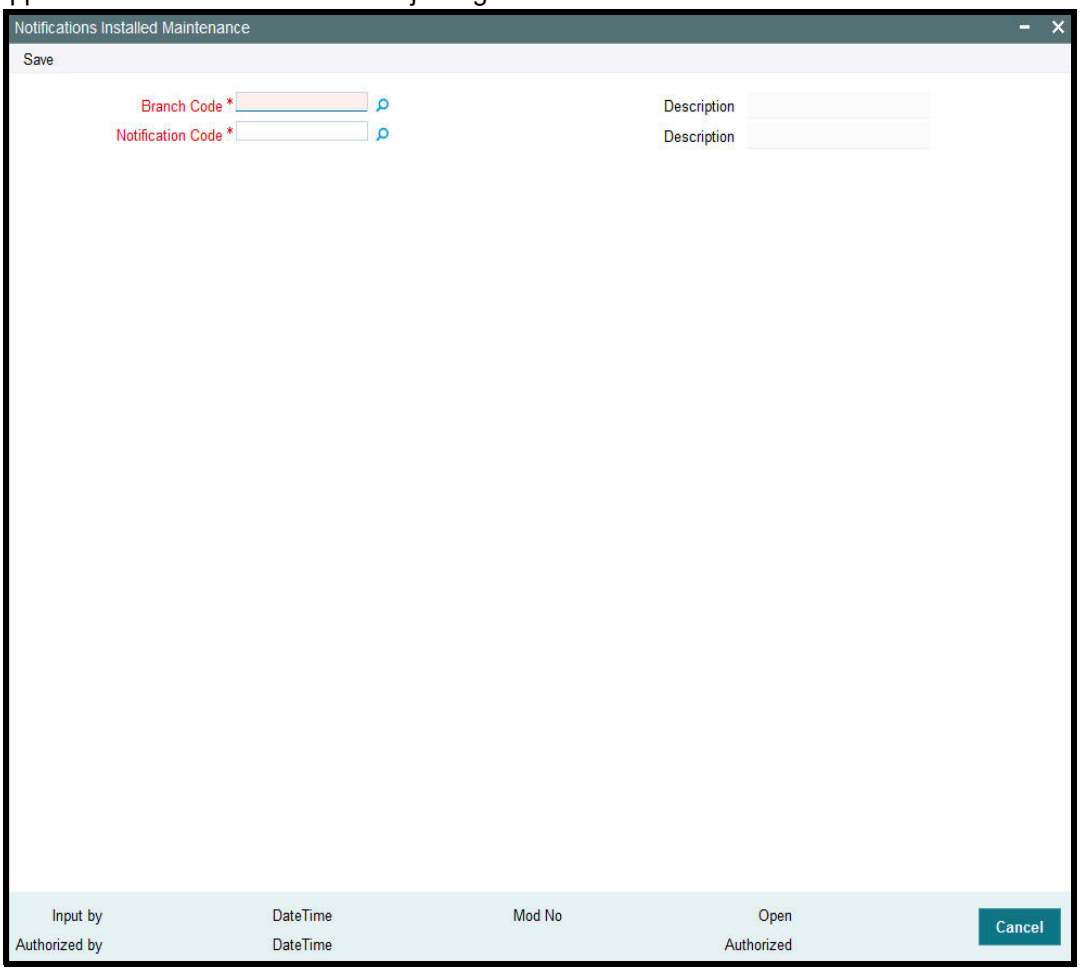
2.15 Notifications Installed Maintenance

This section contains the following topics:

- Section 2.15.1, "Invoking Notifications Installed Maintenance Screen"

2.15.1 Invoking Notifications Installed Maintenance Screen

You can maintain installed notifications using ‘Notifications Installed Maintenance’ screen. You can invoke this screen by typing ‘UTDNTFIN’ in the field at the top right corner of the Application tool bar and click the adjoining arrow.



You can specify the following details:

Branch Code

Alphanumeric; 12 Characters; Mandatory

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

Description

Display

The system displays the description for the selected branch code.

Notification Code

Alphanumeric; 120 Characters; Mandatory

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

Description

Display

The system displays the description for the selected notification code.

2.16 Notifications Installed Summary

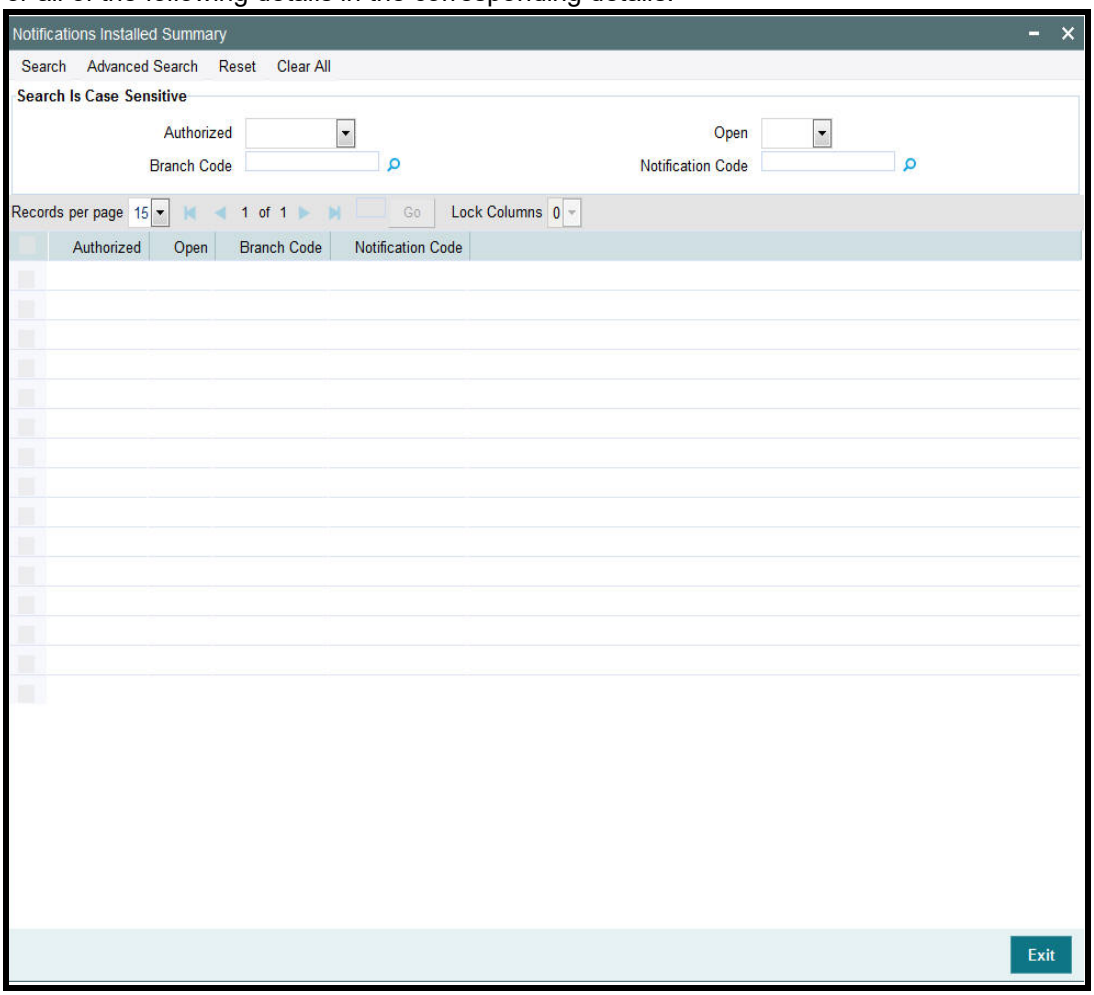
This section contains the following topics:

- Section 2.16.1, "Retrieving a Record in Notifications Installed Summary Screen"
- Section 2.16.2, "Editing Notifications Installed Record"
- Section 2.16.3, "Viewing Notifications Installed Record"
- Section 2.16.4, "Deleting Notifications Installed Record"
- Section 2.16.5, "Authorizing Notifications Installed Record"
- Section 2.16.6, "Amending Notifications Installed Record"
- Section 2.16.7, "Authorizing Amended Notifications Installed Record"

2.16.1 Retrieving a Record in Notifications Installed Summary Screen

You can retrieve a previously entered record in the Summary Screen, as follows:

Invoke the 'Notifications Installed Summary' screen by typing 'UTSNTFIN' in the field at the top right corner of the Application tool bar. Click on the adjoining arrow button and specify any or all of the following details in the corresponding details.



- The status of the record in the Authorized field. If you choose the ‘Blank Space’ option, then all the records are retrieved.
- The status of the record in the Open field. If you choose the ‘Blank Space’ option, then all records are retrieved
- Branch Code
- Notification Code

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

Note

You can also retrieve the individual record detail from the detail screen by querying in the following manner:

- Press F7
- Input the Branch Code
- Press F8

You can perform Edit, Delete, Amend, Authorize, Reverse, Confirm operations by selecting the operation from the Action list. You can also search a record by using a combination of % and alphanumeric value

2.16.2 Editing Notifications Installed Record

You can modify the details of Notifications Installed record that you have already entered into the system, provided it has not subsequently authorized. You can perform this operation as follows:

- Invoke the Notifications Installed Summary screen from the Browser.
- Select the status of the record that you want to retrieve for modification in the Authorized field. You can only modify records that are unauthorized. Accordingly, choose the Unauthorized option.
- Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.
- Click ‘Search’ button. All unauthorized 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 in the list of displayed records. The Notifications Installed Maintenance screen is displayed.
- Select Unlock Operation from the Action list to modify the record. Modify the necessary information.

Click Save to save your changes. The Notifications Installed Maintenance screen is closed and the changes made are reflected in the Notifications Installed Summary screen.

2.16.3 Viewing Notifications Installed Record

To view a record that you have previously input, you must retrieve the same in the Notifications Installed Summary screen as follows:

- Invoke the Notifications Installed Summary screen from the Browser.

- Select the status of the record that you want to retrieve for viewing in the Authorized field. You can also view all records that are either unauthorized or authorized only, by choosing the unauthorized / Authorized option.
- Specify any or all of the details of the record in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to view in the list of displayed records. The Notifications Installed Maintenance screen is displayed in View mode.

2.16.4 Deleting Notifications Installed Record

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

- Invoke the Notifications Installed 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 in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to delete in the list of displayed records. The Notifications Installed Maintenance screen is displayed.
- Select Delete Operation from the Action list. The system prompts you to confirm the deletion and the record is physically deleted from the system database.

2.16.5 Authorizing Notifications Installed Record

- An unauthorized Notifications Installed Maintenance record must be authorized in the system for it to be processed. To authorize a record:
- Invoke the Notifications Installed Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. Typically, choose the unauthorized option.
- Specify any or all of the details in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.
- Double click the record that you wish to authorize. The Notifications Installed Maintenance screen is displayed. Select Authorize operation from the Action List.

When a checker authorizes a record, details of validation, if any, that were overridden by the maker of the record during the Save operation are displayed. If any of these overrides results in an error, the checker must reject the record.

2.16.6 Amending Notifications Installed Record

After a Notifications Installed Maintenance record is authorized, it can be modified using the Unlock operation from the Action List. To make changes to a record after authorization:

- Invoke the Notifications Installed Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. You can only amend authorized records.
- Specify any or all of the details in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.

- Double click the record that you wish to authorize. The Notifications Installed Maintenance screen is displayed in amendment mode. Select Unlock operation from the Action List to amend the record.
- Amend the necessary information and click on Save to save the changes

2.16.7 Authorizing Amended Notifications Installed Record

An amended Notifications Installed Maintenance record must be authorized for the amendment to be made effective in the system. The authorization of amended records can be done only from Fund Manager Module and Agency Branch module.

The subsequent process of authorization is the same as that for normal transactions.

3. Enabling Auto Authorization

This chapter contains the following sections:

3.1 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.

3.2 Auto-authorization

This section contains the following topics:

3.2.1 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 FCIS 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

3.2.2 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 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.

For UT transaction screen, you can derive auto authorization status along with branch, Function ID and User Level Auto Auth Preference using 'Auto Auth' screen. If the Branch, Function ID and menu level auto auth maintenance is derived as 'A' then you should auto authorize a UT Transaction record.

- First priority will be Infra level Auto Auth Derivation [branch, function ID and user level]
- Second priority will be Auto Auth Derivation based on Auto Auth setup maintenance 'SMDAUTAU'
- Third priority will be Auto Auth derivation FBC Access restriction detail 'UTDFAR'

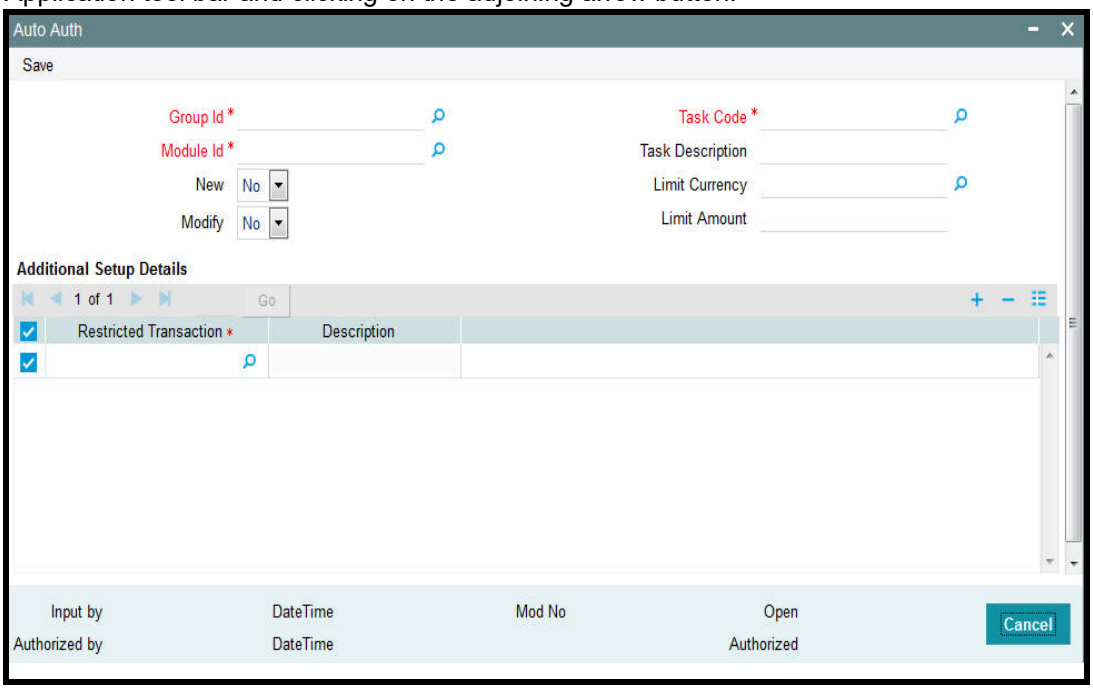
If in all three levels if the auto auth check is returning true, then the system will auto authorize a record.

If there is no maintenance done in FBC Access restriction detail 'UTDFAR', then auto auth check will happen using Infra level Auto Auth Derivation and Auto Auth Setup Maintenance 'SMDAUTAU'.

If there is no maintenance done in Auto Auth Setup Maintenance 'SMDAUTAU', then auto auth check will happen using Infra level Auto Auth Derivation and FBC Access restriction detail.

If there is no maintenance done in Auto Auth Setup Maintenance 'SMDAUTAU' and FBC Access restriction detail 'UTDFAR'. Then auto auth check will happen using Infra level auto auth derivation.

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.



You can specify the following details:

Group Id

Alphanumeric; 15 Characters; Mandatory

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

Module Id

Alphanumeric; 30 Characters; Mandatory

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

New

Optional

Select if the auto authorization is enabled or not for New mode from the drop-down list. The list displays all following values:

- Yes
- No

Modify

Optional

Select if the auto authorization is enabled or not for Modify mode from the drop-down list. The list displays all following values:

- Yes
- No

Task Code

Alphanumeric; 30 Characters; Mandatory

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

Task Description

Display

The system display the description for the selected task code.

Limit Currency

Alphanumeric; 3 Characters; Mandatory

Specify the limit currency code. Alternatively, you can select limit currency code from the option list. The option list displays all valid limit currency code maintained in the system.

Limit Amount

Numeric; 15 Characters; Mandatory

Specify the limit amount.

Additional Setup Details

Restricted Transaction

Numeric; 22 Characters; Mandatory

Specify the restricted transaction code. Alternatively, you can select restricted transaction code from the option list. The option list displays all valid restricted transaction code maintained in the system.

Auto auth setup can be done based on following additional information:

- Backdated Transaction
- Load Overridden Transaction
- Third Party Payment Transaction
- Third Party Delivery Transaction

Description

Display

The system display the description for the selected restricted transaction code.

3.2.2.1 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 access this screen by clicking Security Maintenance menu and selecting Auto Auth from the Browser.

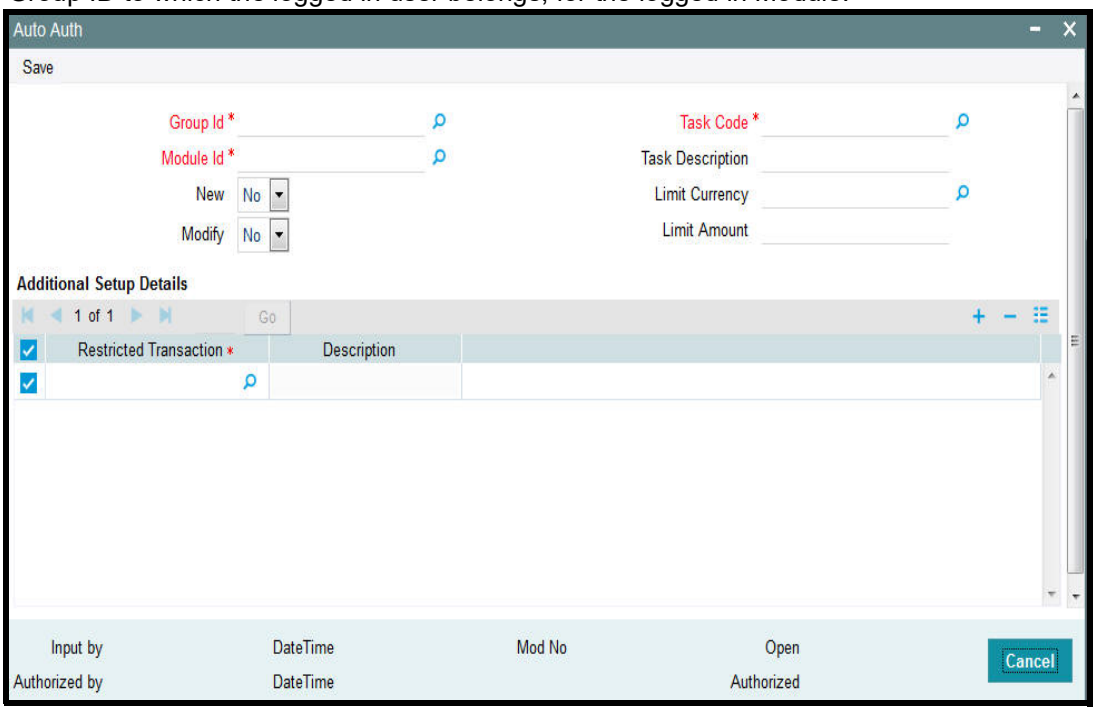
3.2.2.2 Auto Auth Maintenance Screen

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.

3.2.2.3 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.

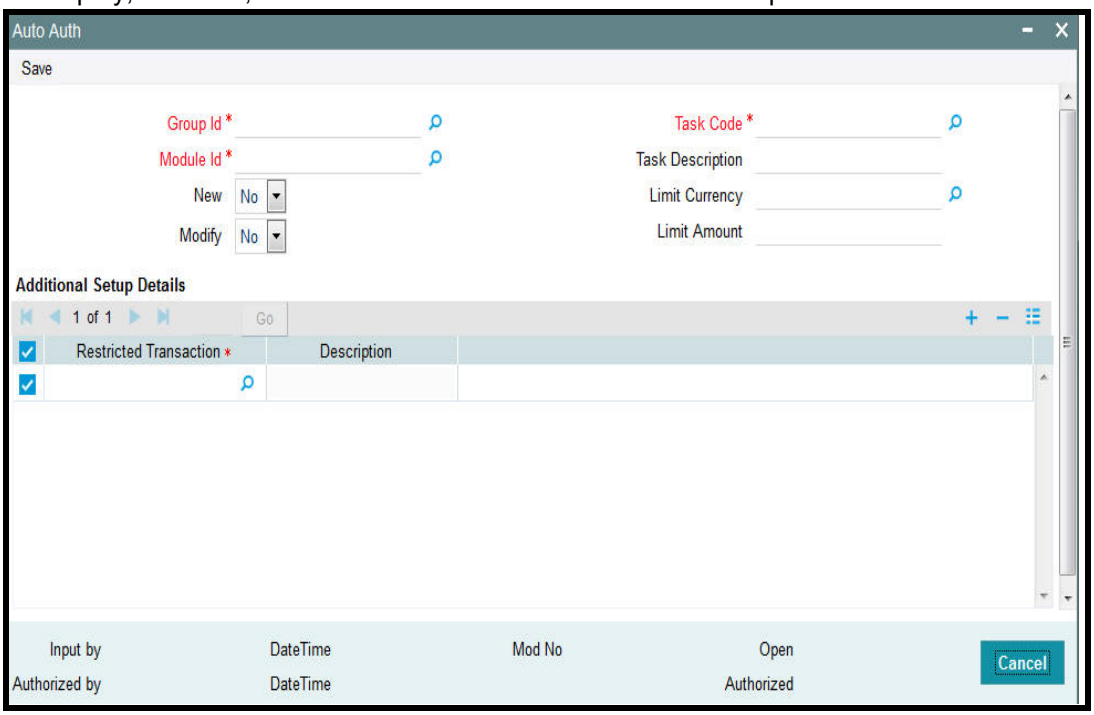


You can make changes as follows:

- To enable auto-authorization in the New mode for a task item, select 'YES' in the New field 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.

Auto auth setup can be done based on additional information like whether transaction is as follows:

- Backdated Transaction
- Load Overridden Transaction
- Third Party Payment Transaction
- Third Party Delivery Transaction

Auto Auth maintenance can be setup based on Fund and RPO code in FBC Access Restriction Detail [UTDFAR] along with Access Restriction Information.

AutoAuthSetuptbl

The auto auth set up table is as follows:

Description	Function Id	Control String	Limit Applicable
Adjustment Subscription	UTDADJ02	101111111	Y
Adjustment Redemption	UTDADJ03	101111111	Y
Block	UTDTXN06	101111111	Y
Consolidation	UTDTXN08	101111111	Y
Switch	UTDTXN04	101111111	Y
Unblock	UTDTXN07	101111111	Y
IPO Subscription	UTDTXN01	101111111	Y
Subscription	UTDTXN02	101111111	Y
Reissue	UTDTXN10	101111111	Y
Redemption	UTDTXN03	101111111	Y
Split	UTDTXN09	101111111	Y
Transfer	UTDTXN05	101111111	Y

AutoAuthAddInfoTbl

The auto auth additional info table is as follows:

Description	Function ID
Adjustment Subscription	UTDADJ02
Adjustment Redemption	UTDADJ03
Block	UTDTXN06
Consolidation	UTDTXN08
Switch	UTDTXN04
Unblock	UTDTXN07
IPO Subscription	UTDTXN01
Subscription	UTDTXN02
Reissue	UTDTXN10
Redemption	UTDTXN03
Split	UTDTXN09
Transfer	UTDTXN05

3.2.3 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 setup:

- Retrieval for viewing
- Editing unauthorized setup
- Deleting unauthorized setup
- Authorizing setup
- Amending authorized setup

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

4. External System Maintenance

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

This chapter contains the following sections:

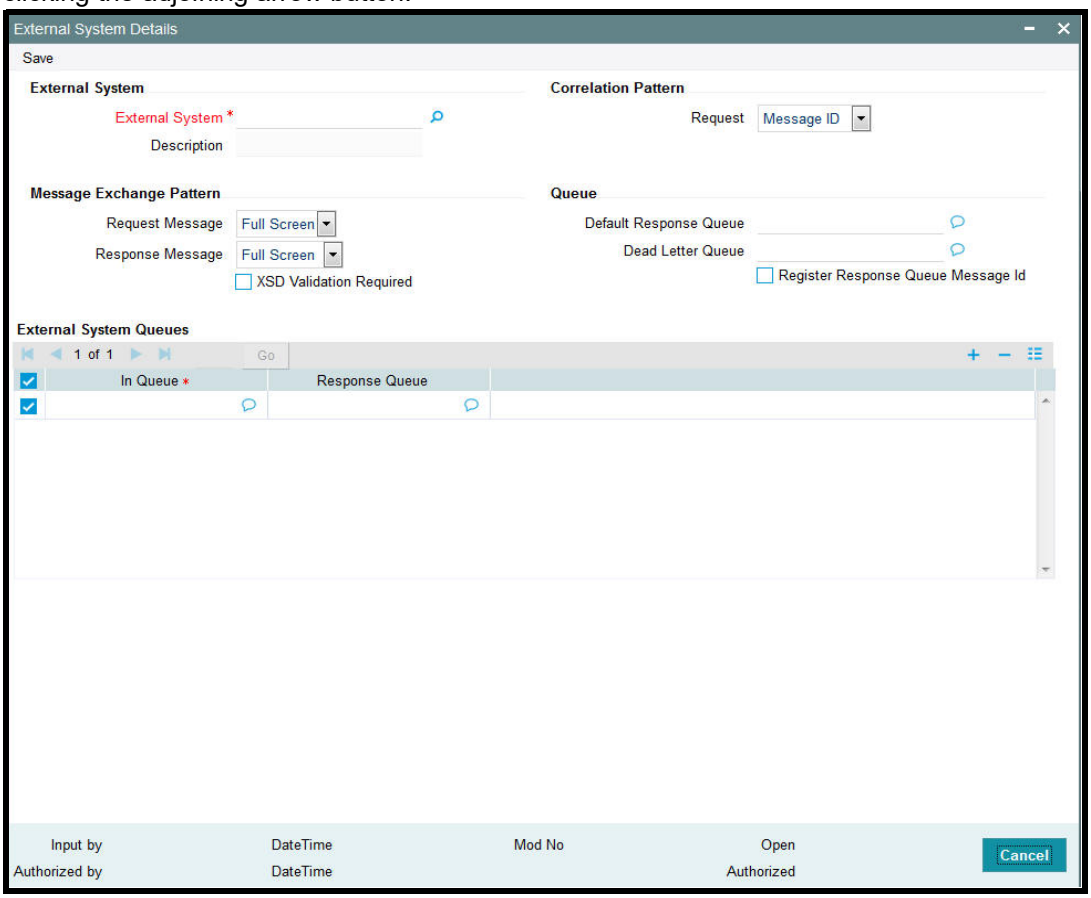
4.1 External System

This section contains the following topics:

4.1.1 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

Display

The system displays the description for the selected External System.

Correlation Pattern

You can maintain the following parameters here:

Request

Optional

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

Optional

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

Optional

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.
- Primary Key – Select if you have selected 'Input Only' for the request message.

XSD Validation Required

Optional

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

Queue

You can maintain the following parameters here:

Default Response Queue

Alphanumeric; 255 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; 255 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'.

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; 255 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; 255 Characters; Optional

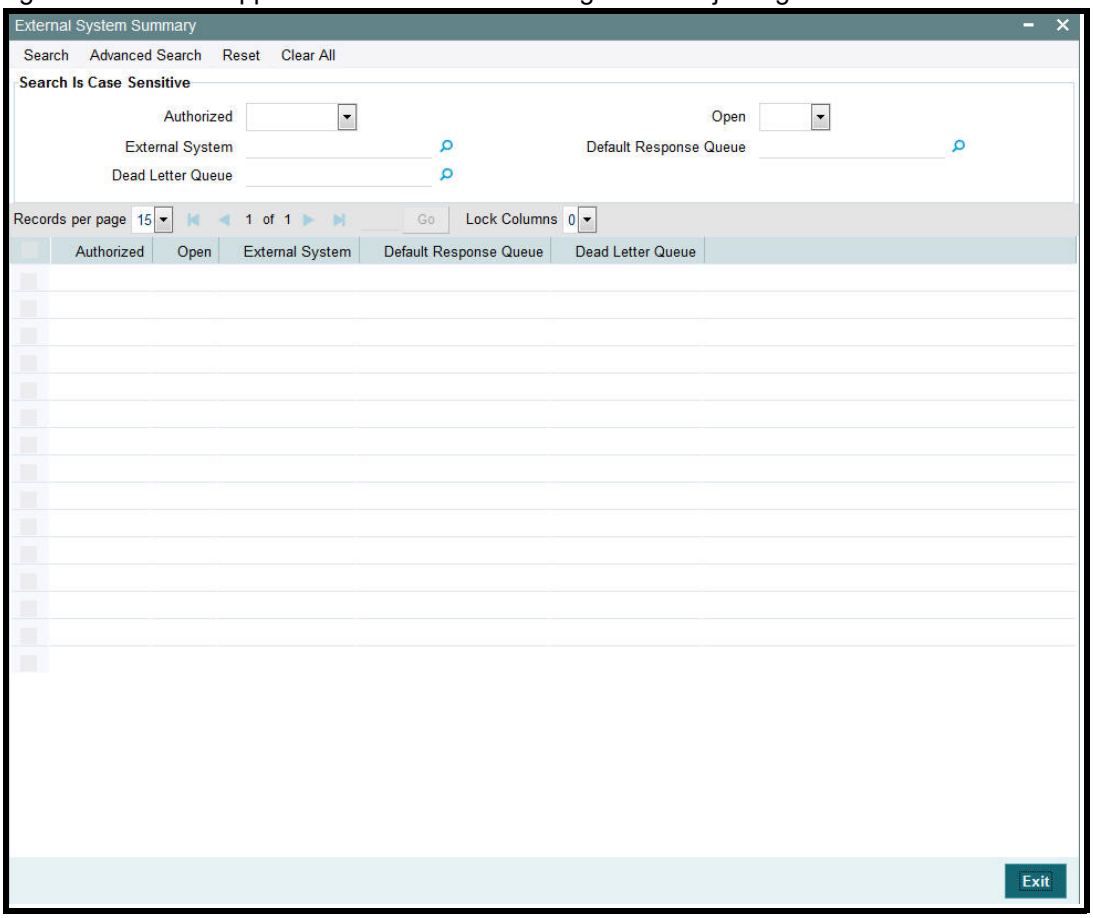
Specify a valid response queue to display the queue name on posting a request message into the In Queue, when the External System fails. Response queue can be maintained for every In Queue.

4.2 External System Summary

This section contains the following topics:

4.2.1 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.

You can retrieve a previously entered stop code in the Summary screen, as follows:

- Invoke the External System Summary screen and specify the following:
  - The status of the fund type in the Authorized field. If you choose the "Blank Space" option, then all the fund types are retrieved.
  - The status of the fund type in the Open field. If you choose the "Blank Space" option, then all the fund types are retrieved.
  - External System
  - Dead Letter Queue
  - Default Response Queue
- After you have specified the required details, click 'Search' button. All Stop codes with the specified details are retrieved and displayed in the lower portion of the screen.

You can also retrieve the stop code detail from the detail screen by doing query in the following manner:-

- Press F7
- Input External System

- Press F8

You can perform Edit, Delete, Amend, Authorize, Reverse, Confirm operation by selecting from the Action list.

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

For example, you can search the record for External System by using the combination of % and alphanumeric value as follows:-

- ***Search by M%***: The system will fetch all the records whose External System starts from Alphabet 'M'. For example, Mutual Fund.
- ***Search by %7*** : The system will fetch all the records whose External System ends by numeric value' 7' For example, 217,267,77 and so forth.
- ***Search by %17%***: The system will fetch all the records whose External System contains the numeric value 17. For example, 3217, 2172 and so forth.

4.2.2 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 Authorized 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.

4.2.3 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.

4.2.4 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.

4.2.5 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.

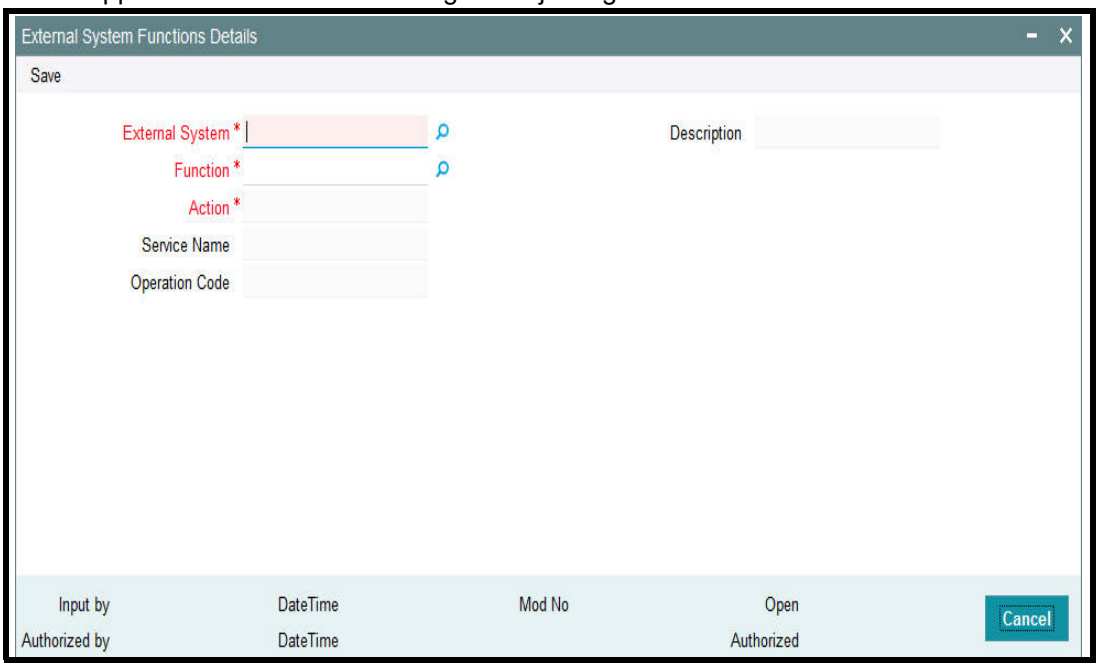
4.3 External System Functions

This section contains the following topics:

- Section 4.3.1, "Maintaining External System Functions"

4.3.1 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

Display

The system displays the description of the specified external system.

Function

Alphanumeric; 8 Characters; Mandatory

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

Action

Display

The system displays an action based on the specified function ID.

Service Name

Display

The system displays the service name based on the specified Function ID and Action.

Operation Code

Display

The system displays Operation Code based on the specified Function ID and Action.

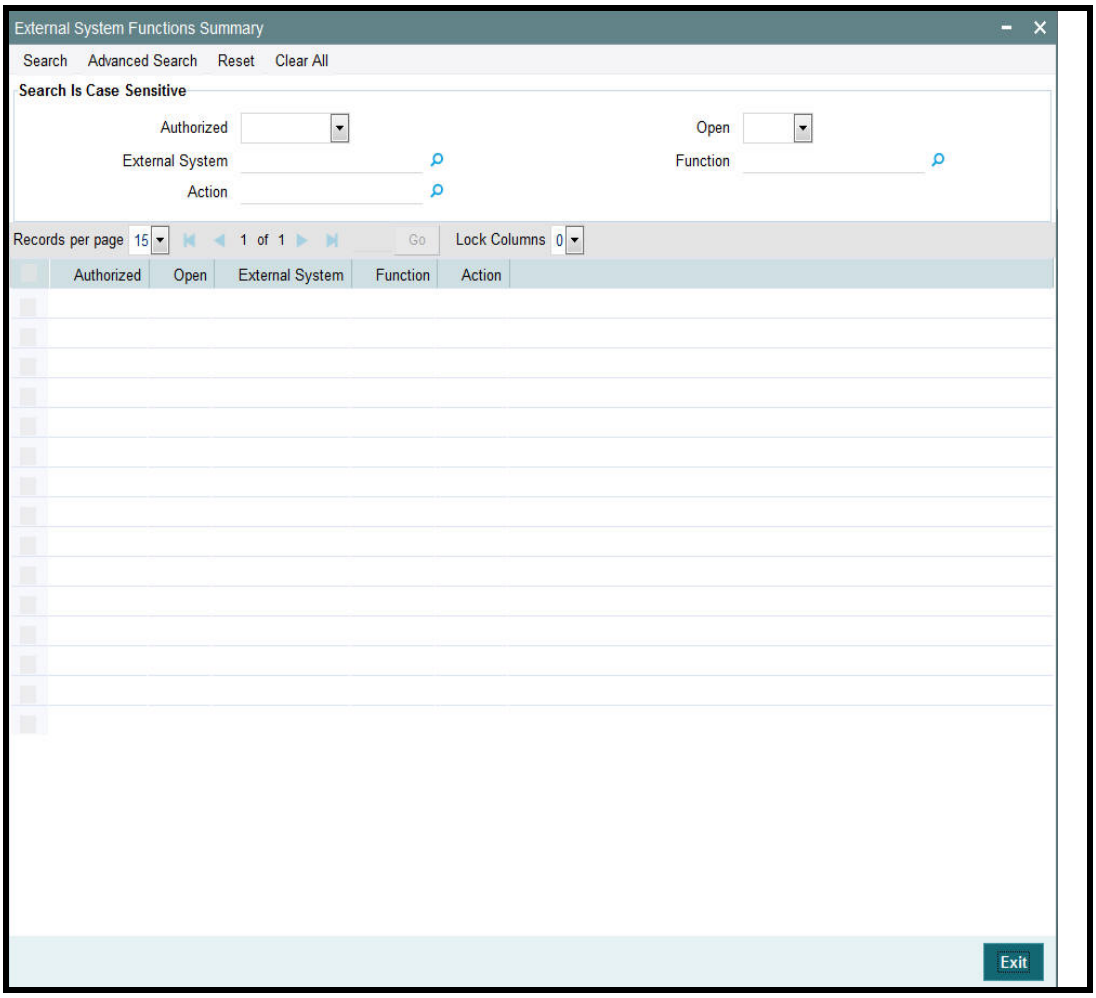
4.4 External System Functions Summary

This section contains the following topics:

4.4.1 Retrieving External System Functions 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.



4.4.2 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 Authorized 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.

4.4.3 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.

4.4.4 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.

4.4.5 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.

4.5 Message Media

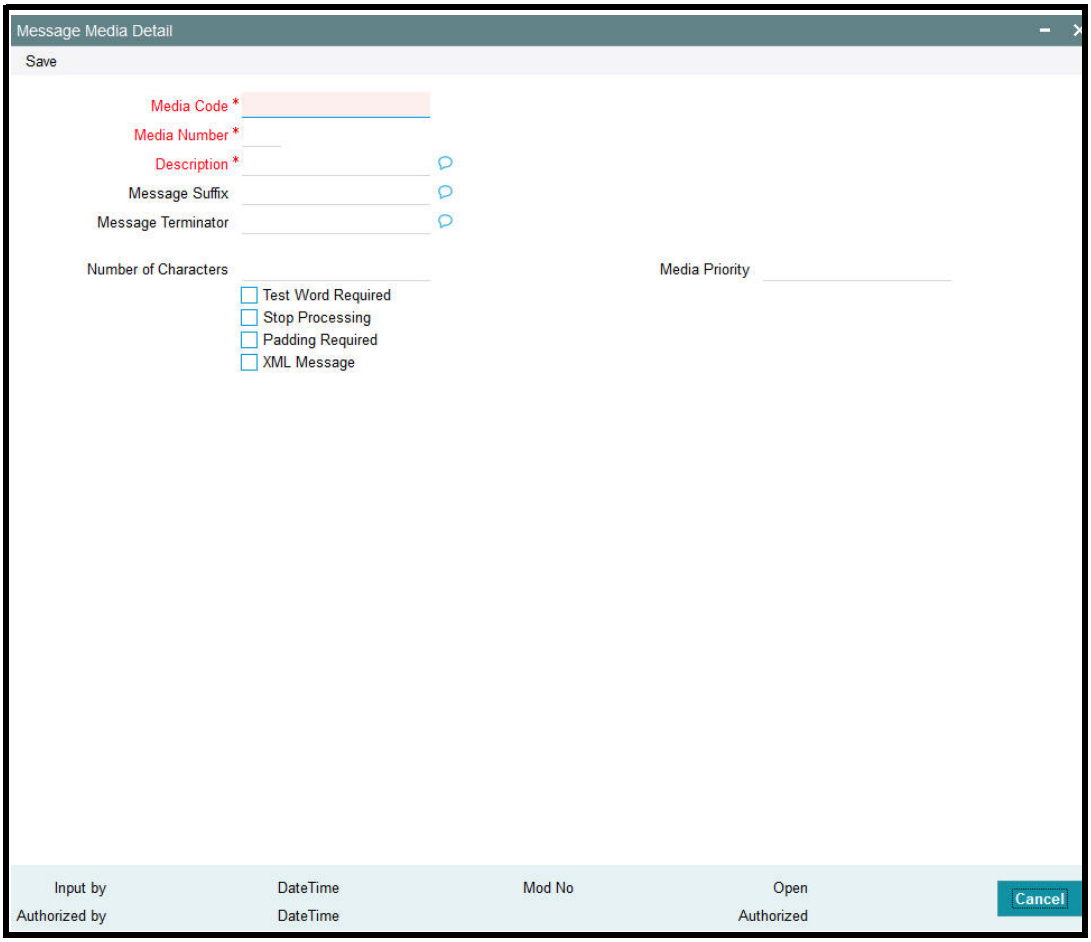
This section contains the following topics:

4.5.1 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; 60 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; 1 Character; Mandatory

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

Description

Alphanumeric; 420 Characters; Mandatory

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

Message Suffix

Alphanumeric; 400 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; 400 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.

XML Message

Optional

Check this box if XML message is required.

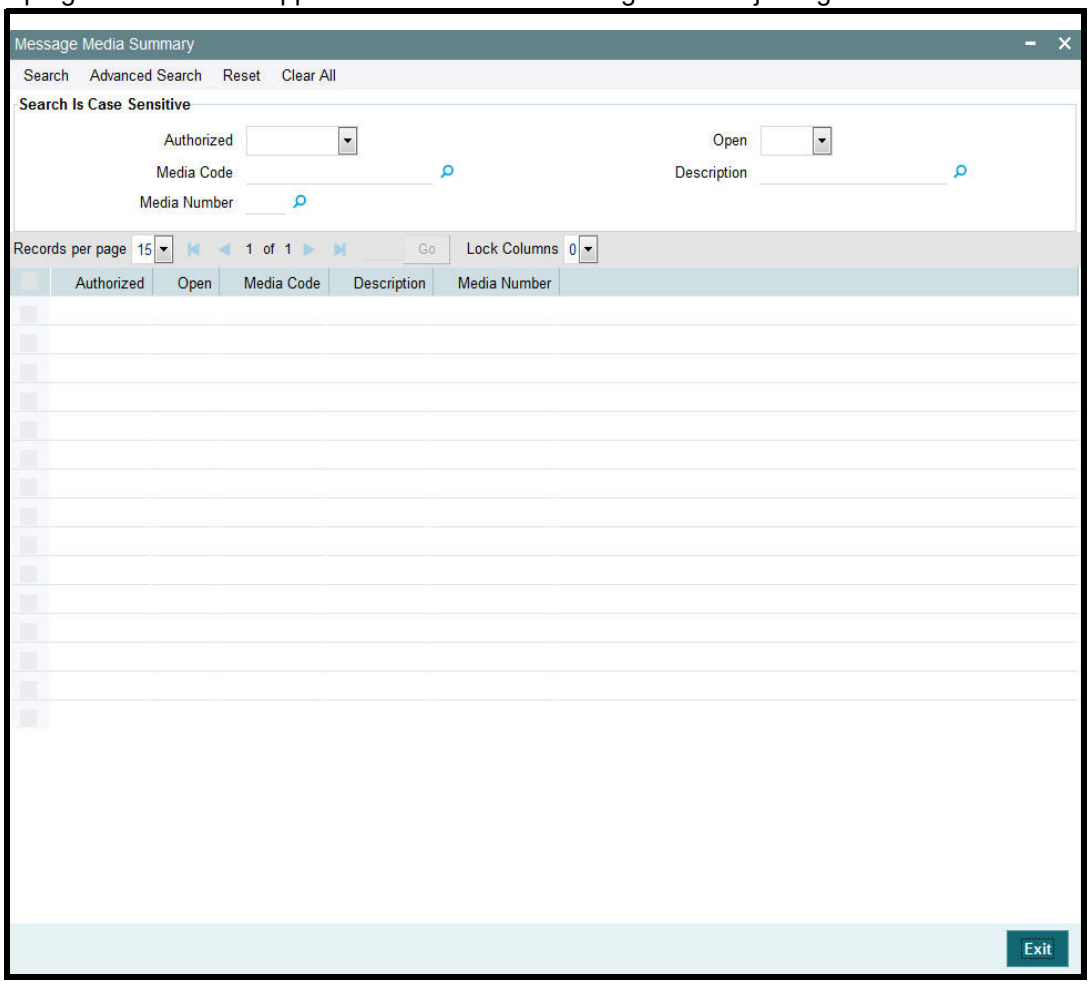
4.6 Message Media Details

This section contains the following topics:

- Section 4.6.3, "Deleting Message Media Details"
- Section 4.6.4, "Modifying Message Media Details"
- Section 4.6.5, "Authorizing Message Media Details"

4.6.1 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

4.6.2 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.

4.6.3 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.

4.6.4 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.

4.6.5 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.

4.7 Media Control System

This section contains the following topics:

- Section 4.7.1, "Maintaining Media Control System"

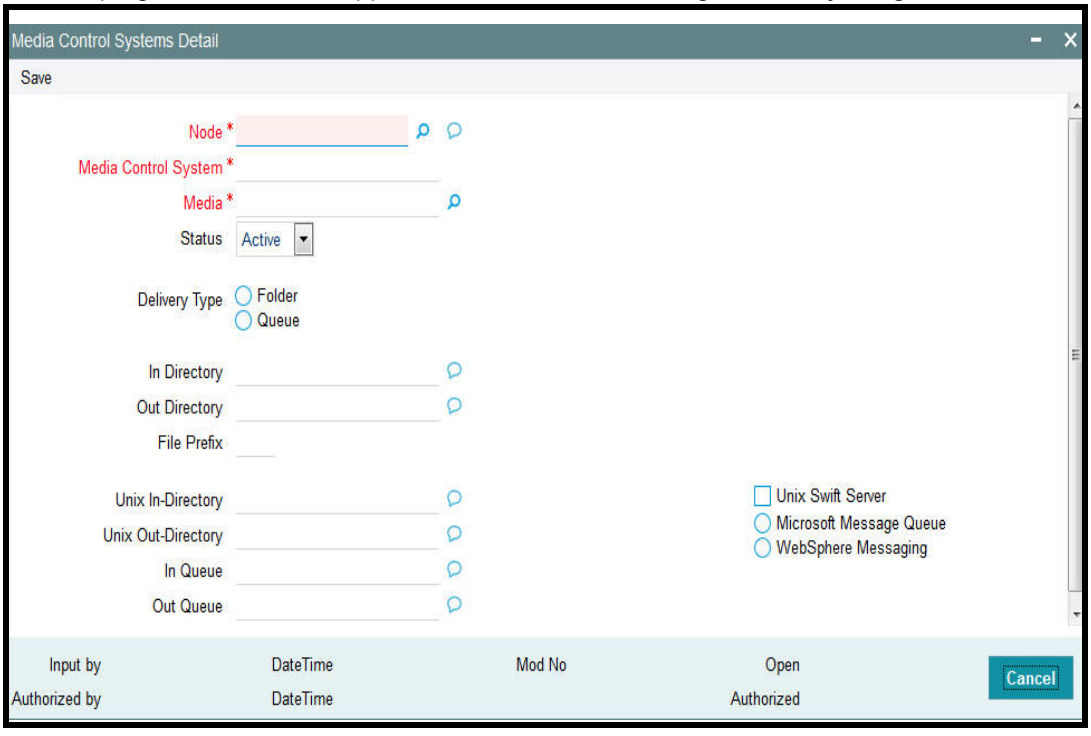
4.7.1 Maintaining Media Control System

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; 420 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; 60 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; 60 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

Optional

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

Optional

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; 512 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; 512 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; 512 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; 512 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; 1020 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; 1020 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.

Microsoft Message Queue

Optional

Check this option to select microsoft message queue.

WebSphere Messaging

Optional

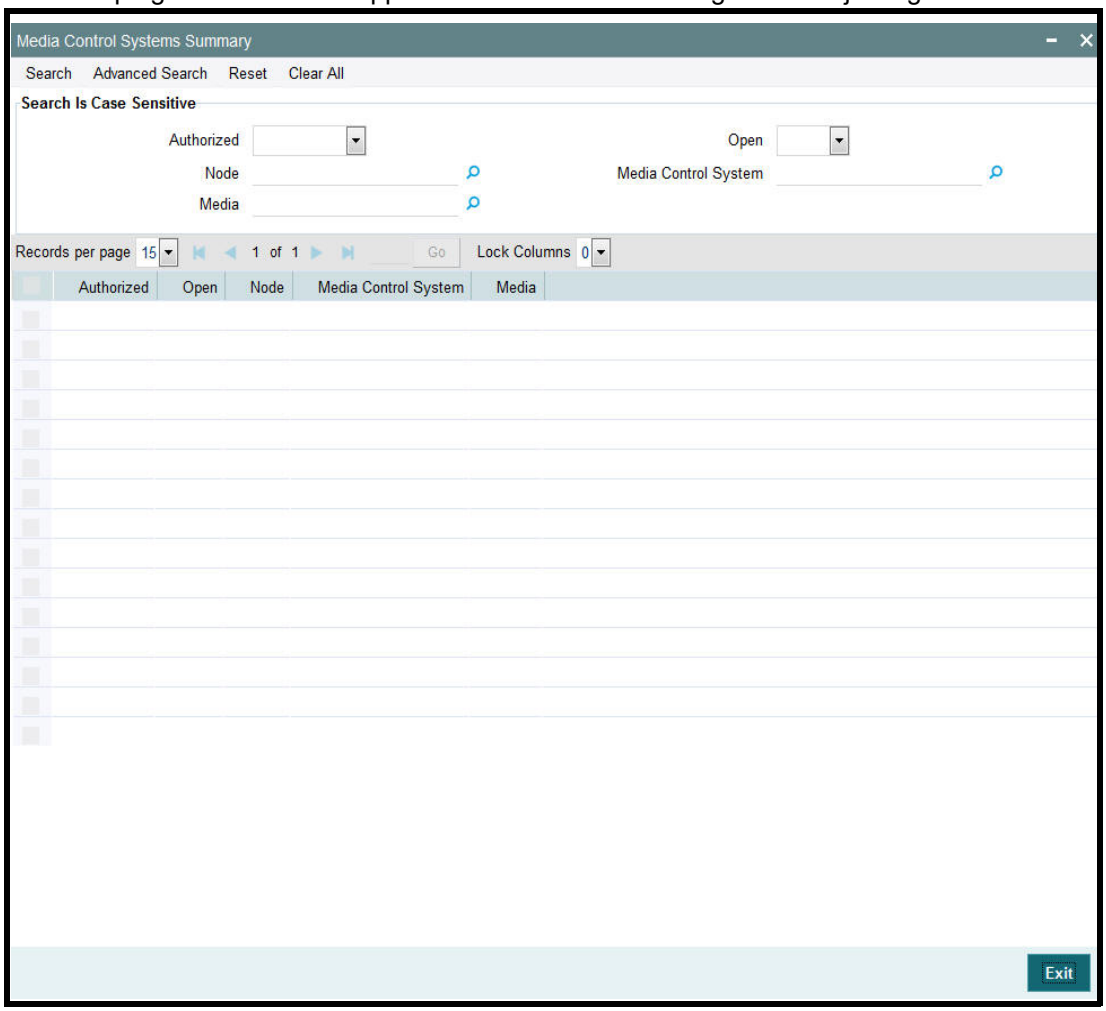
Check this option to select websphere messaging.

4.8 Media Control System Details

This section contains the following topics:

4.8.1 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.

4.8.2 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.

4.8.3 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.

4.8.4 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.

4.8.5 Authorizing Media Control System Details

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

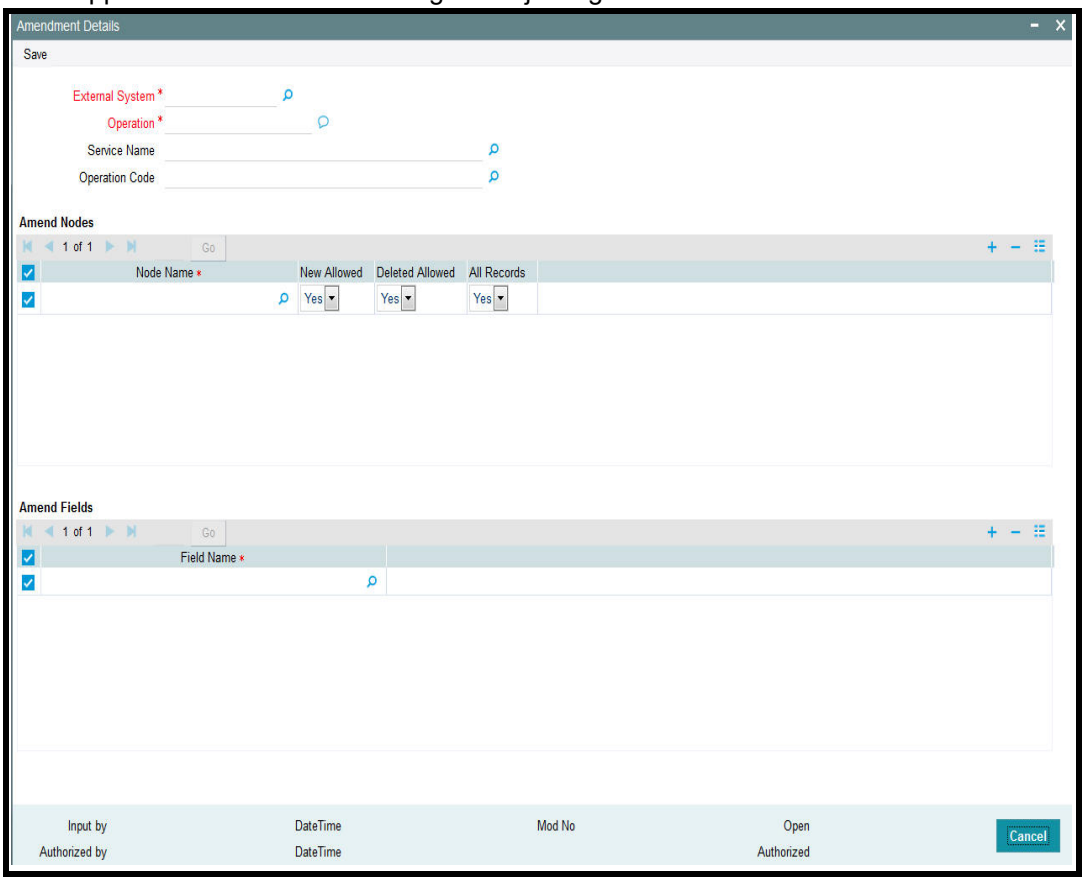
- Invoke the ‘Media Control System Summary’ screen from the Browser.
- Select the status of the record that you want to retrieve for authorization.
- Specify any or all of the details and click ‘Search’ button. All records with the specified details are retrieved and displayed in the lower portion of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

4.9 Amendment Details

This section contains the following topics:

4.9.1 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; 50 Characters; 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

Alphanumeric; 50 Characters; Mandatory

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

New Allowed

Optional

Select whether new records can be added in the node or not from the drop-down list. The list displays the following values:

- Yes
- No

Deleted Allowed

Optional

Select whether existing records can be deleted from the node or not from the drop-down list. The list displays the following values:

- Yes
- No

All Records

Optional

Select if all records had to be amended or not from the drop-down list. The list displays the following values:

- Yes
- No

Amend Fields

Field Name

Alphanumeric; 50 Characters; Optional

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

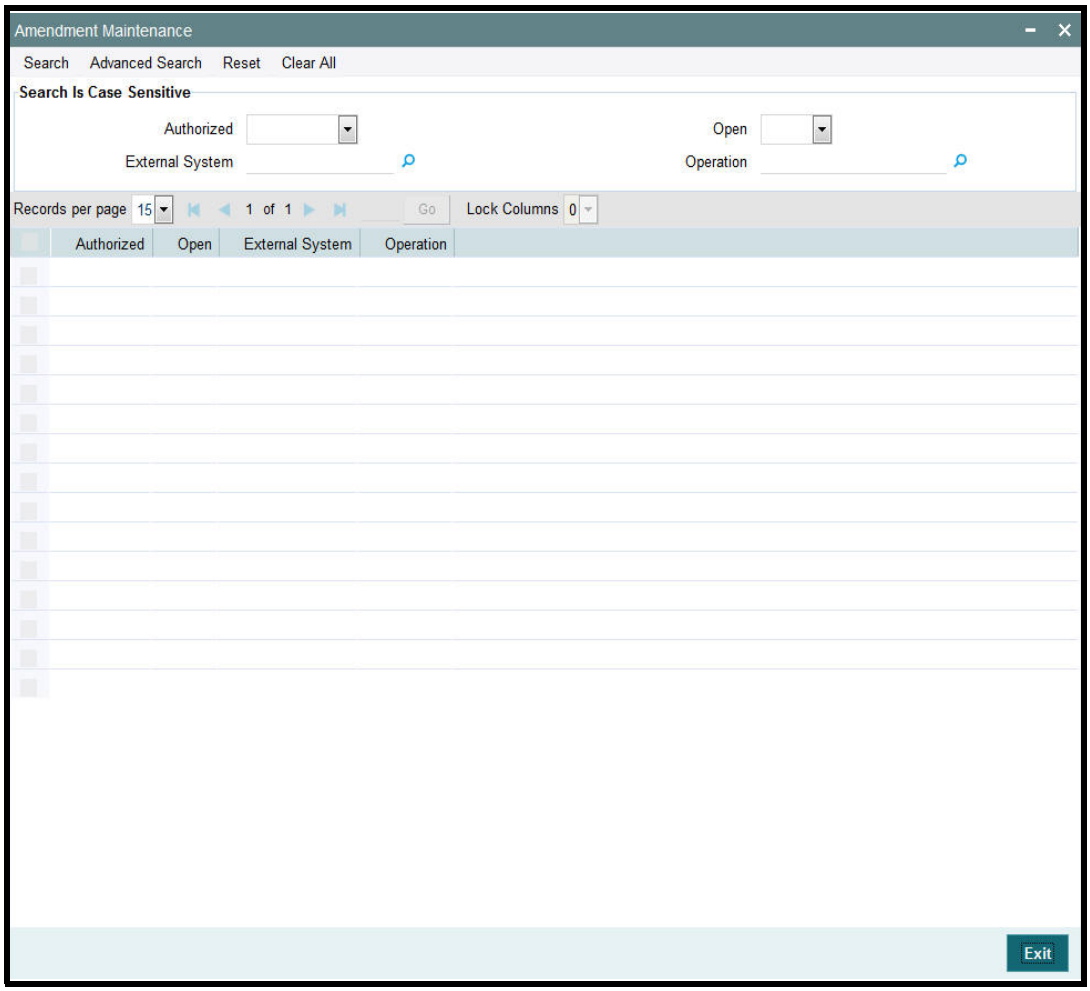
4.10 Amendment Details Retrieval

This section contains the following topics:

4.10.1 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.



4.10.2 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.

4.10.3 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.

4.10.4 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.

4.10.5 Authorizing Amendment Details

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

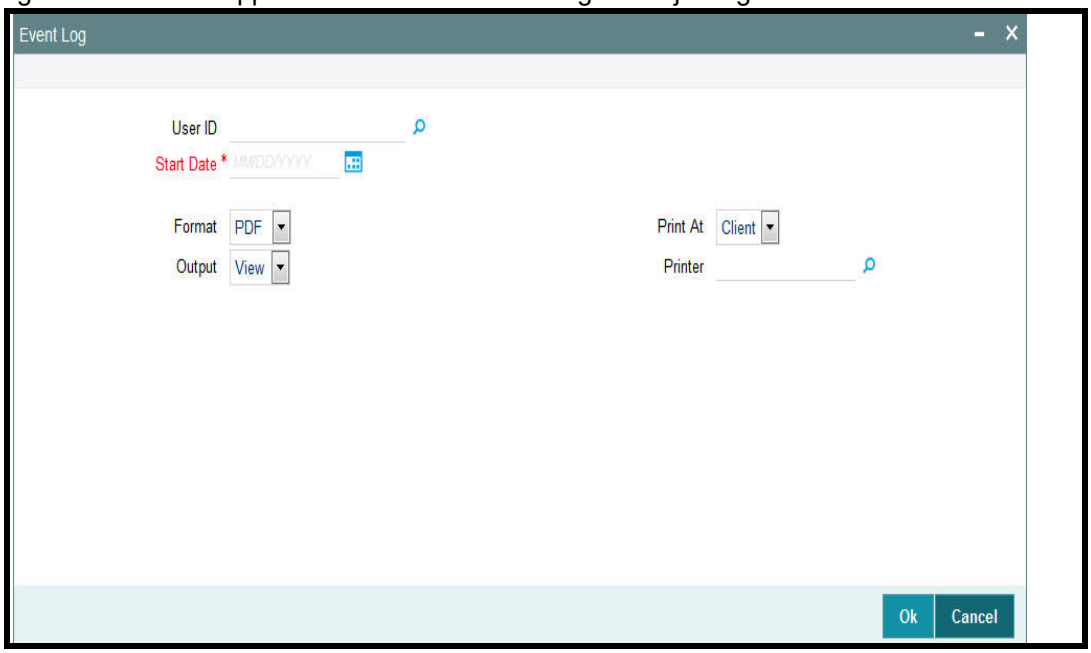
- Invoke the 'Amendment Maintenance Summary' screen from the Browser.
- Select the status of the record that you want to retrieve for authorization.
- Specify any or all of the details and click 'Search' button. All records with the specified details are retrieved and displayed in the lower portion of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

4.11 Events Log

This section contains the following topics:

4.11.1 Invoking Events Log Screen

You can invoke ‘Events’ screen by typing ‘SMREVNLO/ UTREVNLO’ in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.



In this screen, you must specify the following as mandatory parameters for the generation of the report:

User ID

Alphanumeric; 30 Characters; Optional

Specify the user ID. Alternatively, you can select user ID from the option list. The list displays valid user ID maintained in the system.

Start Date

Date Format; Mandatory

Select the start date from the adjoining calendar.

Format

Optional

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

- PDF
- HTML
- Excel
- Excel (.xlsx)
- RTF

Output

Optional

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

- View
- Print
- Spool

Print At

Optional

Select the printing location from the drop-down list. The list displays the following values:

- Client
- Server

Printer

Alphanumeric; 15 Characters; Optional

Specify the printer details from adjoining option list.

The system will generate the event logs after specifying the mandatory details.

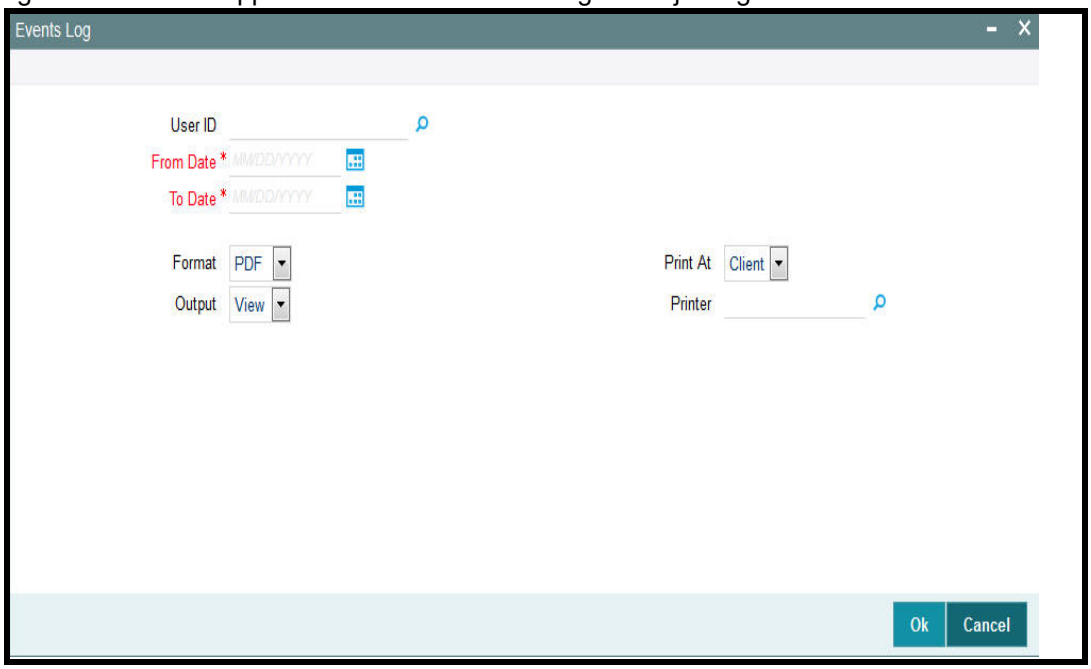
4.12 Events Log

This section contains the following topics:

- Section 4.12.1, "Invoking Events Log Screen"

4.12.1 Invoking Events Log Screen

You can invoke 'Events' screen by typing 'SMRPEVLG/ UTRPEVLG' in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.



In this screen, you must specify the following as mandatory parameters for the generation of the report:

User ID

Alphanumeric; 30 Characters; Optional

Specify the user ID. Alternatively, you can select user ID from the option list. The list displays valid user ID maintained in the system.

From Date and To Date

Date Format; Mandatory

Select the From and To date from the adjoining calendar.

Format

Optional

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

- PDF
- HTML
- Excel
- Excel (.xlsx)
- RTF

Output

Optional

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

- View
- Print
- Spool

Print At

Optional

Select the printing location from the drop-down list. The list displays the following values:

- Client
- Server

Printer

Alphanumeric; 15 Characters; Optional

Specify the printer details from adjoining option list.

The system will generate the event logs after specifying the mandatory details.

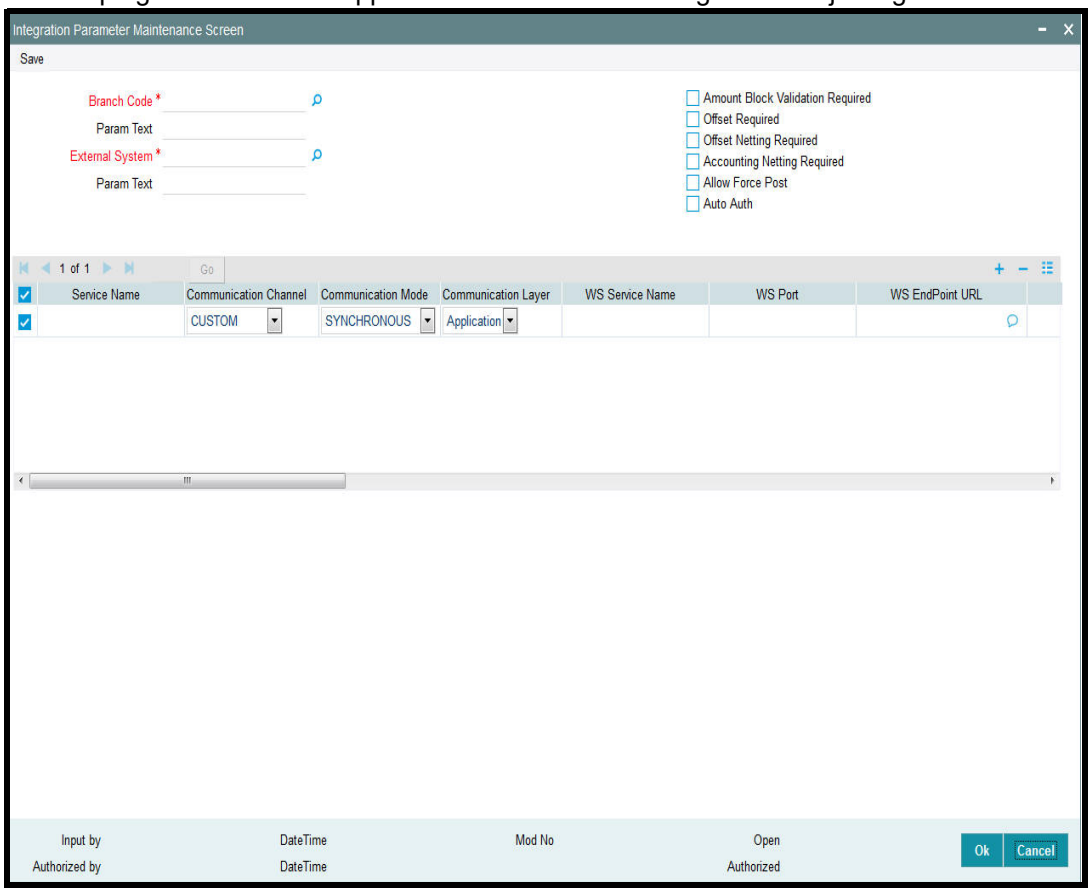
4.13 Integration Parameter Maintenance Screen

This section contains the following topic:

- Section 4.13.1, "Invoking Integration Parameter Maintenance Screen"

4.13.1 Invoking Integration Parameter Maintenance Screen

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



You can specify the following details:

Branch Code

Alphanumeric; 3 Characters; Mandatory

Specify the branch code. Alternatively, you can select the branch code from the option list. The list display all valid branch code maintained in the system.

Param Text

Display

The system displays the description for the selected branch code.

External System

Alphanumeric; 50 Characters; Mandatory

Specify the external system details. Alternatively, you can select the external system details from the option list. The list display all valid external system details maintained in the system.

Param Text

Display

The system displays the description for the selected external system.

Amount Block Validation Required

Optional

Check this box if amount block validation is required.

Offset Required

Optional

Check this box if offset is required.

Offset Netting Required

Optional

Check this box if offset netting is required.

Accounting Netting Required

Optional

Check this box if accounting netting is required.

Allow Force Post

Optional

Check this box if force post is allowed.

Auto Auth

Optional

Check this box if auto authorization is required.

Service Name

Alphanumeric; 100 Characters; Mandatory

Specify the service name.

Communication Channel

Optional

Select the communication channel from the drop-down list. The list displays the following values:

- Custom
- Webservice
- MDB
- Internal

Communication Mode

Optional

Select the communication mode from the drop-down list. The list displays the following values:

- Synchronous
- Asynchronous

Communication Layer

Optional

Select the communication layer from the drop-down list. The list displays the following values:

- Application
- Database

WS Service Name

Alphanumeric; 250 Characters; Optional

Specify WS Service Name.

WS Port

Numeric; 250 Characters; Optional

Specify WS Port.

WS EndPoint URL

Alphanumeric; 500 Characters; Optional

Specify WS EndPoint URL.

WS User

Alphanumeric; 128 Characters; Optional

Specify WS User.

WS Password

Alphanumeric; 128 Characters; Optional

Specify WS Password.

Custom Classname

Alphanumeric; 255 Characters; Optional

Specify Custom Classname.

ATM Server IP

Numeric; 50 Characters; Optional

Specify the ATM server IP address.

ATM Server Port

Numeric; 50 Characters; Optional

Specify ATM Server Port.

MDB QCF

Alphanumeric; 255 Characters; Optional

Specify MDB QCF details.

MDB Out Queue

Alphanumeric; 255 Characters; Optional

Specify MDB out queue details

MDB Response Queue

Alphanumeric; 255 Characters; Optional

Specify MDB response queue details.

Audit Enabled

Alphanumeric; 2 Characters; Optional

Specify audit enabled details.

Source

Alphanumeric; 20 Characters; Optional

Specify source details.

External DataSource

Alphanumeric; 50 Characters; Optional

Specify external data source details.

Symmetric Key

Alphanumeric; 50 Characters; Optional

Specify symmetric key details.

4.14 Upload Source Maintenance

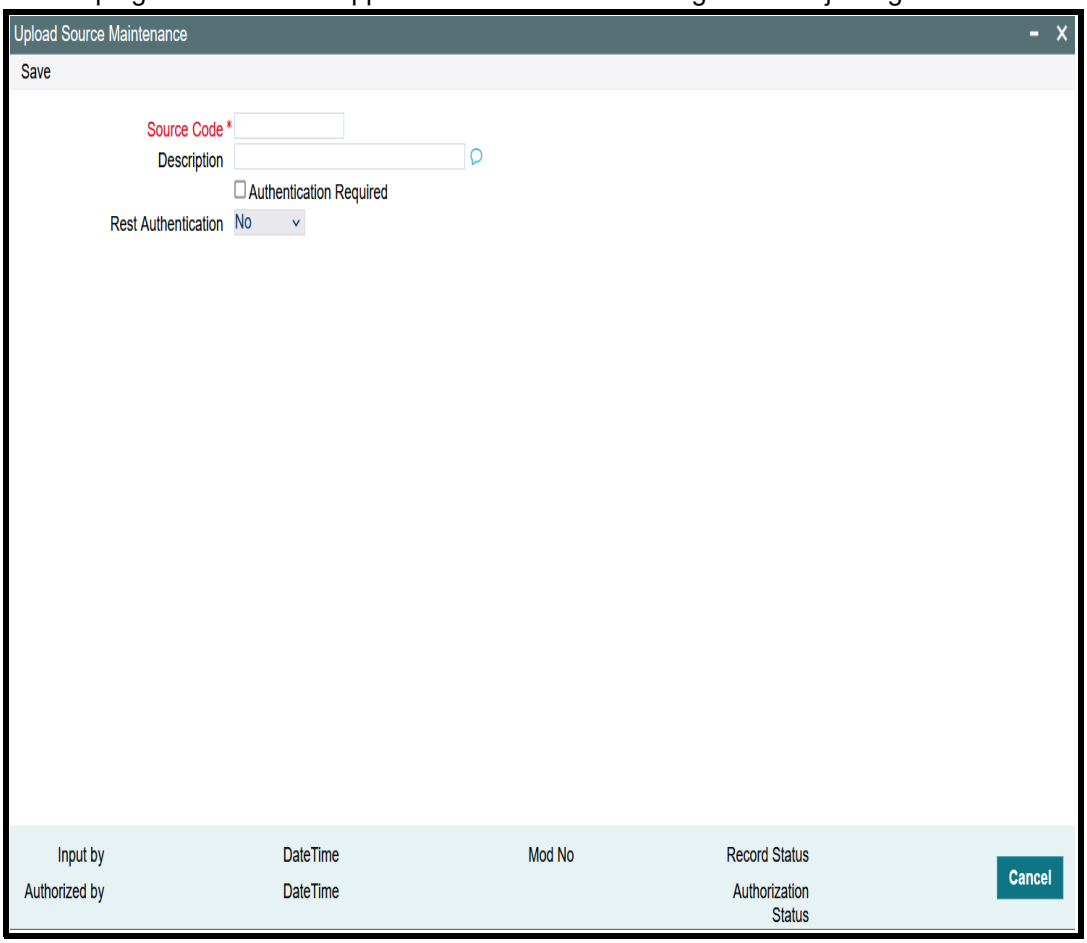
This section contains the following topic:

- Section 4.14.1, "Invoking Upload Source Maintenance Screen"

4.14.1 Invoking Upload Source Maintenance Screen

Oracle FLEXCUBE Investor Servicing facilitates upload of data from an external source. The details of the source from which data has to be uploaded need to be maintained in Oracle FLEXCUBE Investor Servicing using the 'Upload Source Maintenance' screen.

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



You can specify the following details.

Source Code

Alphanumeric; 15 Characters; Mandatory

Specify a source code from which data has to be uploaded to Oracle FLEXCUBE Investor Servicing.

Description

Alphanumeric; 105 Characters; Mandatory

Specify the description for the source code specified.

Authentication Required

Optional

Check this box to indicate if base data has to be uploaded from Oracle FLEXCUBE Investor Servicing.

Rest Authentication

Optional

This field is applicable only for REST service. Default value of this field will be 'No'.You can choose to do any of the following:

- No - Select this option not to perform any User password Authentication
- Flexcube - Select this option to authenticate the User password based on Flexcube user data
- JWT - Select this option to authenticate the User based on JWT maintenance

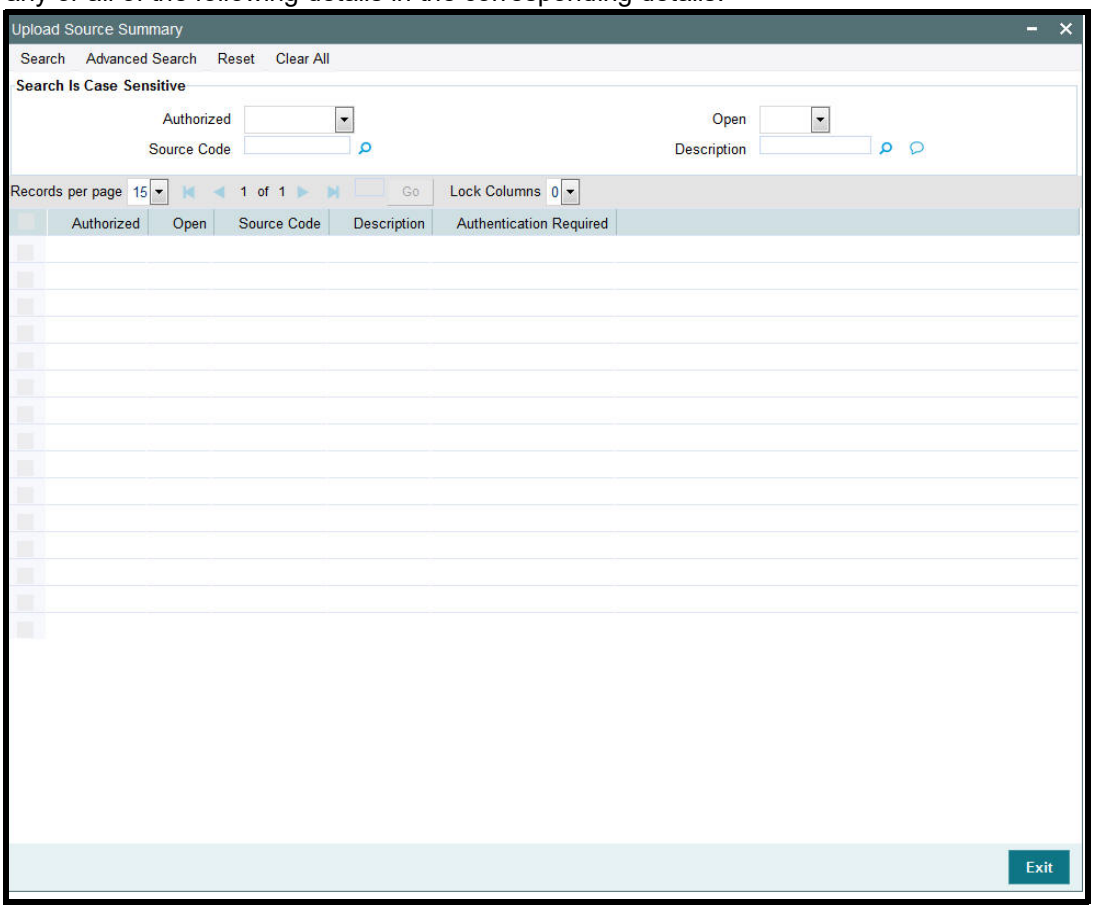
4.15 Upload Source Summary

This section contains the following topic:

4.15.1 Retrieving a Record in Upload Source Summary Screen

You can retrieve a previously entered record in the Summary Screen, as follows:

Invoke the ‘Upload Source Summary’ screen by typing ‘SMSSORCE’ in the field at the top right corner of the Application tool bar and clicking on the adjoining arrow button and specify any or all of the following details in the corresponding details.



- The status of the record in the Authorized field. If you choose the ‘Blank Space’ option, then all the records are retrieved.
- The status of the record in the Open field. If you choose the ‘Blank Space’ option, then all records are retrieved
- Source Code
- Description

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

Note

You can also retrieve the individual record detail from the detail screen by querying in the following manner:

- Press F7
- Input the Source Code
- Press F8

You can perform Edit, Delete, Amend, Authorize, Reverse, Confirm operations by selecting the operation from the Action list. You can also search a record by using a combination of % and alphanumeric value

4.15.2 Editing Upload Source Record

You can modify the details of Upload Source record that you have already entered into the system, provided it has not subsequently authorized. You can perform this operation as follows:

- Invoke the Upload Source Summary screen from the Browser.
- Select the status of the record that you want to retrieve for modification in the Authorized field. You can only modify records that are unauthorized. Accordingly, choose the Unauthorized option.
- Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.
- Click 'Search' button. All unauthorized 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 in the list of displayed records. The Upload Source Maintenance screen is displayed.
- Select Unlock Operation from the Action list to modify the record. Modify the necessary information.

Click Save to save your changes. The Upload Source Maintenance screen is closed and the changes made are reflected in the Upload Source Summary screen.

4.15.3 Viewing Upload Source Record

To view a record that you have previously input, you must retrieve the same in the Upload Source Summary screen as follows:

- Invoke the Upload Source Summary screen from the Browser.
- Select the status of the record that you want to retrieve for viewing in the Authorized field. You can also view all records that are either unauthorized or authorized only, by choosing the unauthorized / Authorized option.
- Specify any or all of the details of the record in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to view in the list of displayed records. The Upload Source Maintenance screen is displayed in View mode.

4.15.4 Deleting Upload Source Record

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

- Invoke the Upload Source 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 in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to delete in the list of displayed records. The Upload Source Maintenance screen is displayed.
- Select Delete Operation from the Action list. The system prompts you to confirm the deletion and the record is physically deleted from the system database.

4.15.5 Authorizing Upload Source Record

- An unauthorized Upload Source record must be authorized in the system for it to be processed. To authorize a record:
- Invoke the Upload Source Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. Typically, choose the unauthorized option.
- Specify any or all of the details in the corresponding fields on the screen.
- Click ‘Search’ button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.
- Double click the record that you wish to authorize. The Upload Source Maintenance screen is displayed. Select Authorize operation from the Action List.

When a checker authorizes a record, details of validation, if any, that were overridden by the maker of the record during the Save operation are displayed. If any of these overrides results in an error, the checker must reject the record.

4.15.6 Amending Upload Source Record

After a Upload Source record is authorized, it can be modified using the Unlock operation from the Action List. To make changes to a record after authorization:

- Invoke the Upload Source Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. You can only amend authorized records.
- Specify any or all of the details in the corresponding fields on the screen.
- Click ‘Search’ button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.
- Double click the record that you wish to authorize. The Upload Source Maintenance screen is displayed in amendment mode. Select Unlock operation from the Action List to amend the record.
- Amend the necessary information and click on Save to save the changes

4.15.7 Authorizing Amended Upload Source Record

An amended Upload Source record must be authorized for the amendment to be made effective in the system. The authorization of amended records can be done only from Fund Manager Module and Agency Branch module.

The subsequent process of authorization is the same as that for normal transactions.

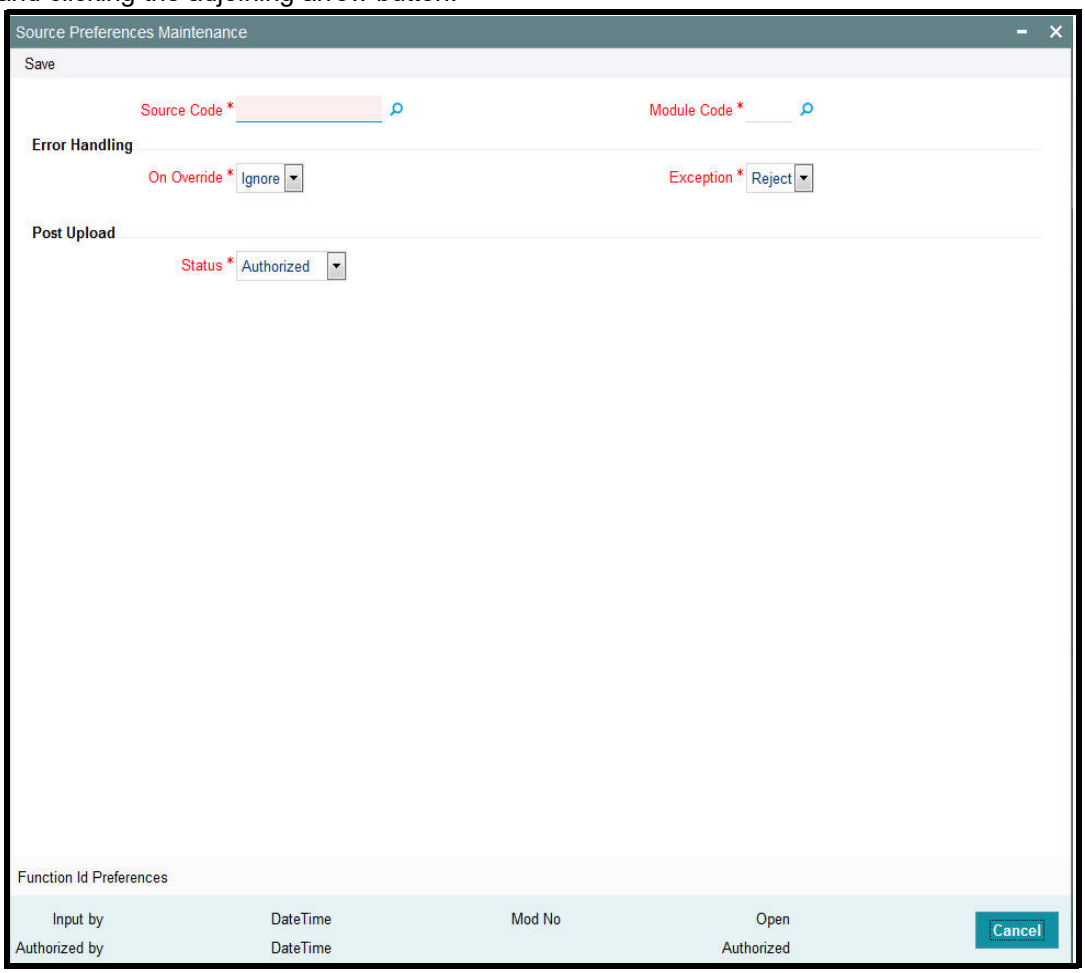
4.16 Source Preferences Maintenance

This section contains the following topic:

4.16.1 Invoking Source Preferences Maintenance Screen

You can set preferences for upload of data from an external source in the ‘Source Preferences Maintenance’ screen. You can invoke the ‘Source Preferences Maintenance’

screen by typing ‘SMDUPLDM’ in the field at the top right corner of the Application tool bar and clicking the adjoining arrow button.



The following details are captured here:

Source Code

Alphanumeric; 15 Characters; Mandatory

Select Source Code from the option list. Depending on the source code you select here data is uploaded from that source into Oracle FLEXCUBE IS.

Module Code

Alphanumeric; 2 Characters; Mandatory

You can choose to upload data from a source directly onto a module in Oracle FLEXCUBE IS. Indicate the module into which you would like to upload data from a given source.

Error Handling

On Override

Mandatory

Oracle FLEXCUBE IS generates override messages in case it encounters any discrepancies during data upload. You can choose to do any of the following:

- Ignore – Select this option to ignore such error messages and continue with the upload process
- Reject – Select this option to reject the record

Exception

Mandatory

In case a serious error occurs during data upload, Oracle FLEXCUBE IS generates an error message. You can choose to put the record with the error on hold. If you would like to reject the record altogether, choose 'Reject' from the drop-down list.

Post Upload

Status

Mandatory

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

- Authorized
- Unauthorized

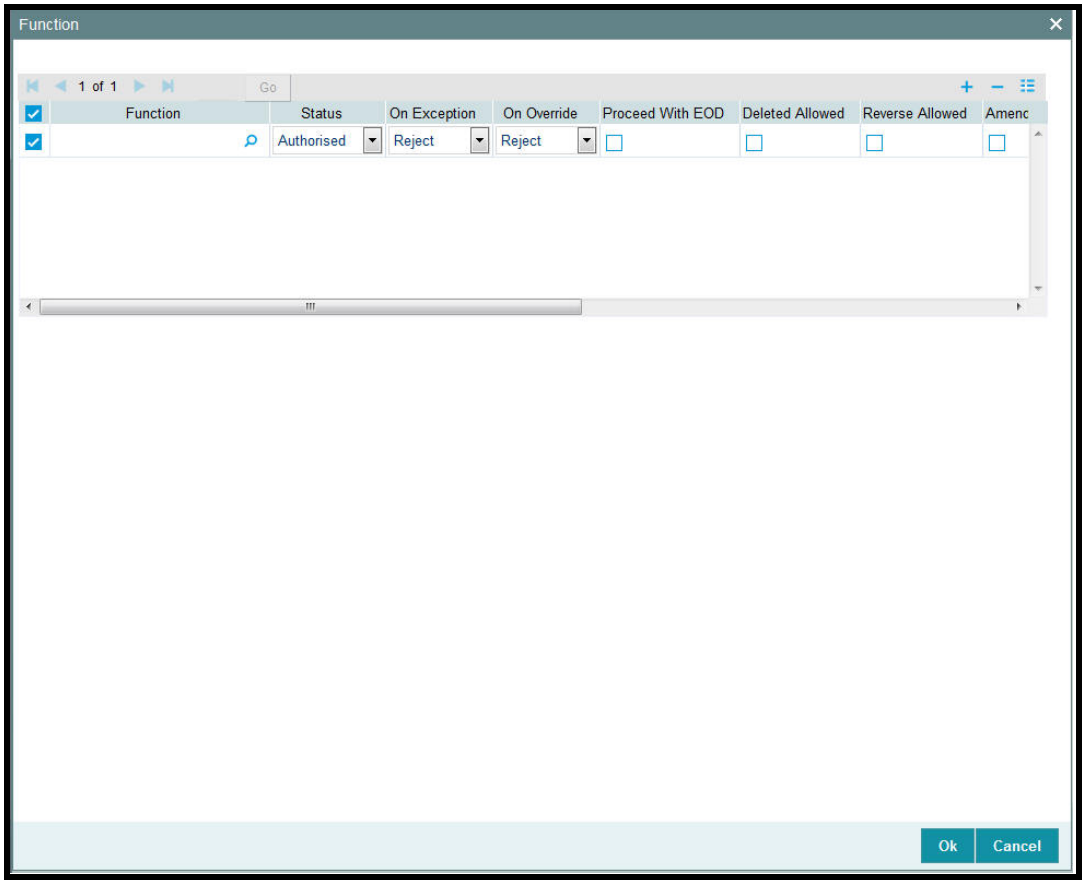
If you would like to automatically authorize the data that is uploaded into Oracle FLEXCUBE choose the 'Authorize' option here.

If you would like the record to be put on hold choose this option in this field.

If you would like the record to be unauthorized, choose the 'Unauthorized' option in this field. The record will not be authorized automatically on upload. You will have to manually authorize the data.

4.16.2 Function ID Preferences Button

Click 'Function ID Preferences' button in 'Source Preferences Maintenance' screen.



You can specify the following details:

Function

Alphanumeric; 8 Characters; Optional

Specify the function ID. Alternatively, you can also select function ID from the option list. The system displays all valid function IDs maintained in the system.

Status

Optional

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

- Authorised
- Unauthorised

On Exception

Optional

Select the on exception details from the drop-down list. The list displays the following values:

- Reject
- Put on Hold

On Override

Optional

Select the on override details from the drop-down list. The list displays the following values:

- Reject
- Put on Hold
- Ignore

Proceed With EOD

Optional

Check this box to proceed with EOD.

Deleted Allowed

Optional

Check this box if deletion of a record is allowed.

Reverse Allowed

Optional

Check this box if reversal of a record is allowed.

Amend Allowed

Optional

Check this box if amending a record is allowed.

Purge Days

Numeric; 4 Characters; Optional

Specify the number of days to be purged.

Allow Deffered Processing

Optional

Check this box to allow deferred processing.

Allow EOD With Deffered

Optional

Check this box to allow EOD with deferred record.

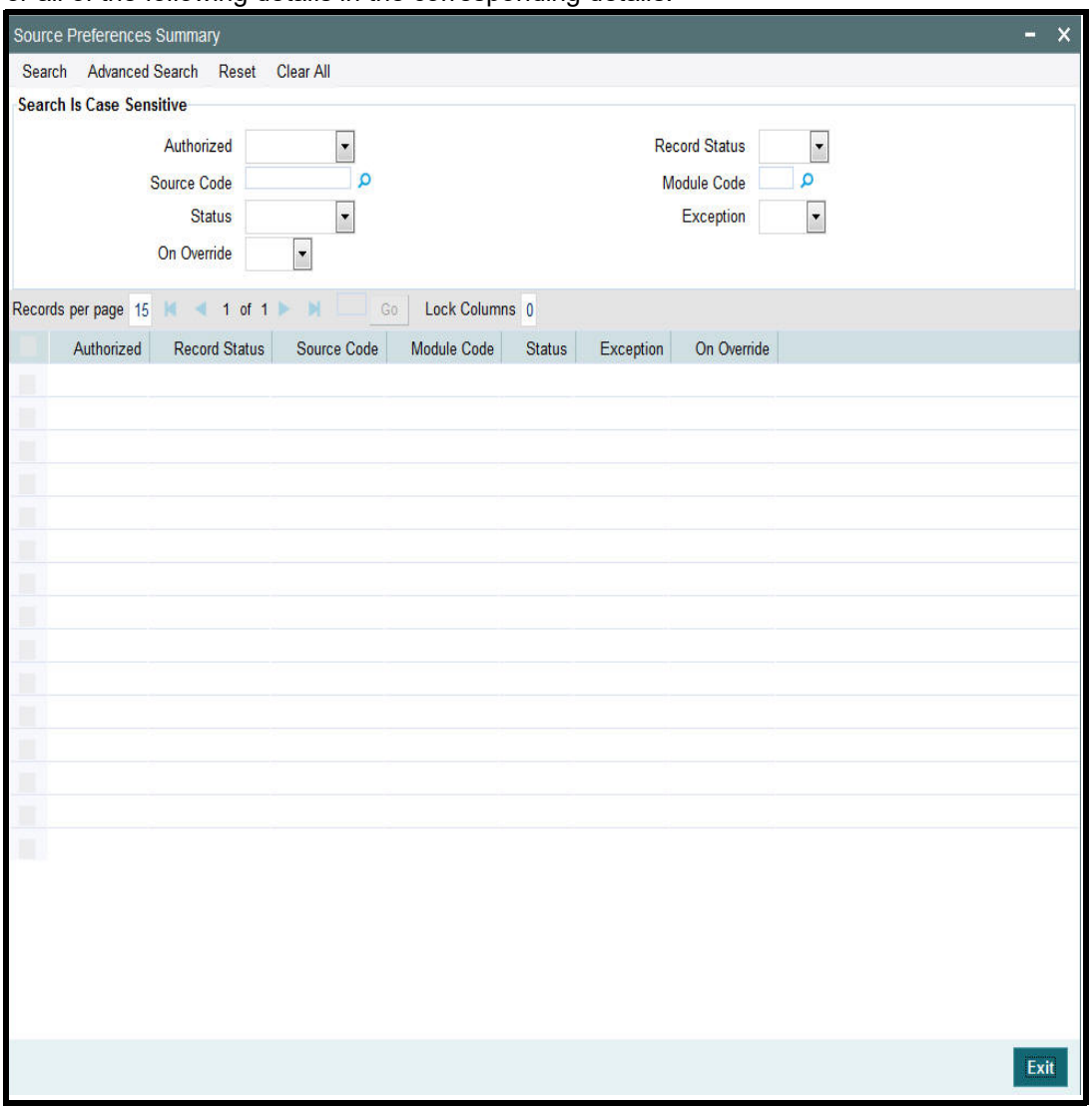
4.17 Source Preferences Summary

This section contains the following topics:

4.17.1 Retrieving a Record in Source Preferences Summary Screen

You can retrieve a previously entered record in the Summary Screen, as follows:

Invoke the ‘Source Preferences Summary’ screen by typing ‘SMSUPLDM’ in the field at the top right corner of the Application tool bar. Click on the adjoining arrow button and specify any or all of the following details in the corresponding details.



- The status of the record in the Authorized field. If you choose the ‘Blank Space’ option, then all the records are retrieved.
- The status of the record in the Record Status field. If you choose the ‘Blank Space’ option, then all records are retrieved
- Source Code
- Status
- On Override
- Module Code
- Exception

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

Note

You can also retrieve the individual record detail from the detail screen by querying in the following manner:

- Press F7
- Input the Source Code
- Press F8

You can perform Edit, Delete, Amend, Authorize, Reverse, Confirm operations by selecting the operation from the Action list. You can also search a record by using a combination of % and alphanumeric value

4.17.2 Editing Source Preference Record

You can modify the details of Source Preferences record that you have already entered into the system, provided it has not subsequently authorized. You can perform this operation as follows:

- Invoke the Source Preferences Summary screen from the Browser.
- Select the status of the record that you want to retrieve for modification in the Authorized field. You can only modify records that are unauthorized. Accordingly, choose the Unauthorized option.
- Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.
- Click 'Search' button. All unauthorized 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 in the list of displayed records. The Source Preferences Maintenance screen is displayed.
- Select Unlock Operation from the Action list to modify the record. Modify the necessary information.

Click Save to save your changes. The Source Preferences Maintenance screen is closed and the changes made are reflected in the Source Preferences Summary screen.

4.17.3 Viewing Source Preferences Record

To view a record that you have previously input, you must retrieve the same in the Source Preferences Summary screen as follows:

- Invoke the Source Preferences Summary screen from the Browser.
- Select the status of the record that you want to retrieve for viewing in the Authorized field. You can also view all records that are either unauthorized or authorized only, by choosing the unauthorized / Authorized option.
- Specify any or all of the details of the record in the corresponding fields on the screen.
- Click 'Search' button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to view in the list of displayed records. The Source Preferences Maintenance screen is displayed in View mode.

4.17.4 Deleting Source Preferences Record

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

- Invoke the Source Preferences 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 in the corresponding fields on the screen.
- Click ‘Search’ button. All records with the specified fields are retrieved and displayed in the lower portion of the screen.
- Double click the record that you want to delete in the list of displayed records. The Source Preferences Maintenance screen is displayed.
- Select Delete Operation from the Action list. The system prompts you to confirm the deletion and the record is physically deleted from the system database.

4.17.5 Authorizing Source Preferences Record

- An unauthorized Source Preferences record must be authorized in the system for it to be processed. To authorize a record:
- Invoke the Source Preferences Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. Typically, choose the unauthorized option.
- Specify any or all of the details in the corresponding fields on the screen.
- Click ‘Search’ button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.
- Double click the record that you wish to authorize. The Source Preferences Maintenance screen is displayed. Select Authorize operation from the Action List.

When a checker authorizes a record, details of validation, if any, that were overridden by the maker of the record during the Save operation are displayed. If any of these overrides results in an error, the checker must reject the record.

4.17.6 Amending Source Preferences Record

After a Source Preferences record is authorized, it can be modified using the Unlock operation from the Action List. To make changes to a record after authorization:

- Invoke the Source Preferences Summary screen from the Browser.
- Select the status of the record that you want to retrieve for authorization. You can only amend authorized records.
- Specify any or all of the details in the corresponding fields on the screen.
- Click ‘Search’ button. All records with the specified details that are pending authorization are retrieved and displayed in the lower portion of the screen.
- Double click the record that you wish to authorize. The Source Preferences Maintenance screen is displayed in amendment mode. Select Unlock operation from the Action List to amend the record.
- Amend the necessary information and click on Save to save the changes

4.17.7 Authorizing Amended Source Preferences Record

An amended Source Preferences record must be authorized for the amendment to be made effective in the system. The authorization of amended records can be done only from Fund Manager Module and Agency Branch module.

The subsequent process of authorization is the same as that for normal transactions.

4.18 Notification Enroute Maintenance

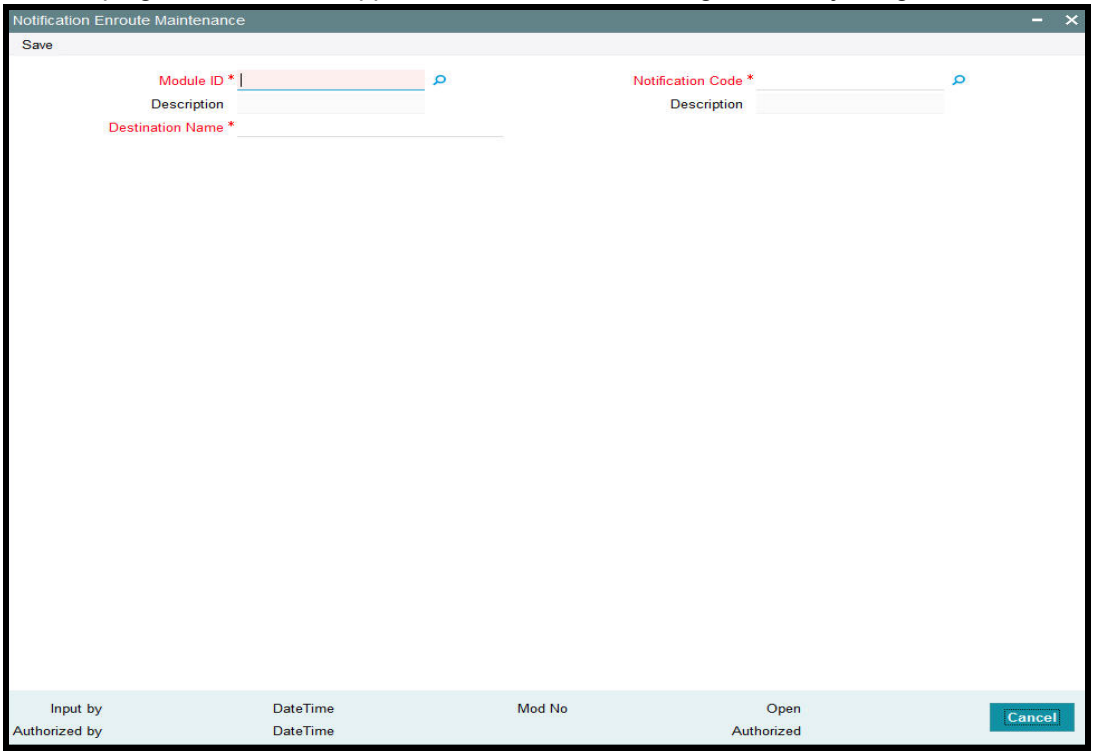
This section contains the following topics:

- Section 4.18.1, "Invoking Notification Enroute Maintenance Screen"

4.18.1 Invoking Notification Enroute Maintenance Screen

You can set up notification queue at module level using 'Notification Enroute Maintenance' screen. Notification job will look into the SMS data store for any pending activity and depending upon the module code call will be made to respective LOB to build response xml and place it in the maintained notification queue for that module.

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



You can specify the following details:

Module ID

Alphanumeric; 30 Characters; Mandatory

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

Description

Display

The system displays the description for the selected module ID.

Notification Code

Alphanumeric; 30 Characters; Mandatory

Specify the notification code. Alternatively, you can select modification code from the option list. The list displays all valid notification code maintained in the system.

Description

Display

The system displays the description for the selected notification code.

Destination Name

Alphanumeric; 100 Characters; Mandatory

Specify the destination name.

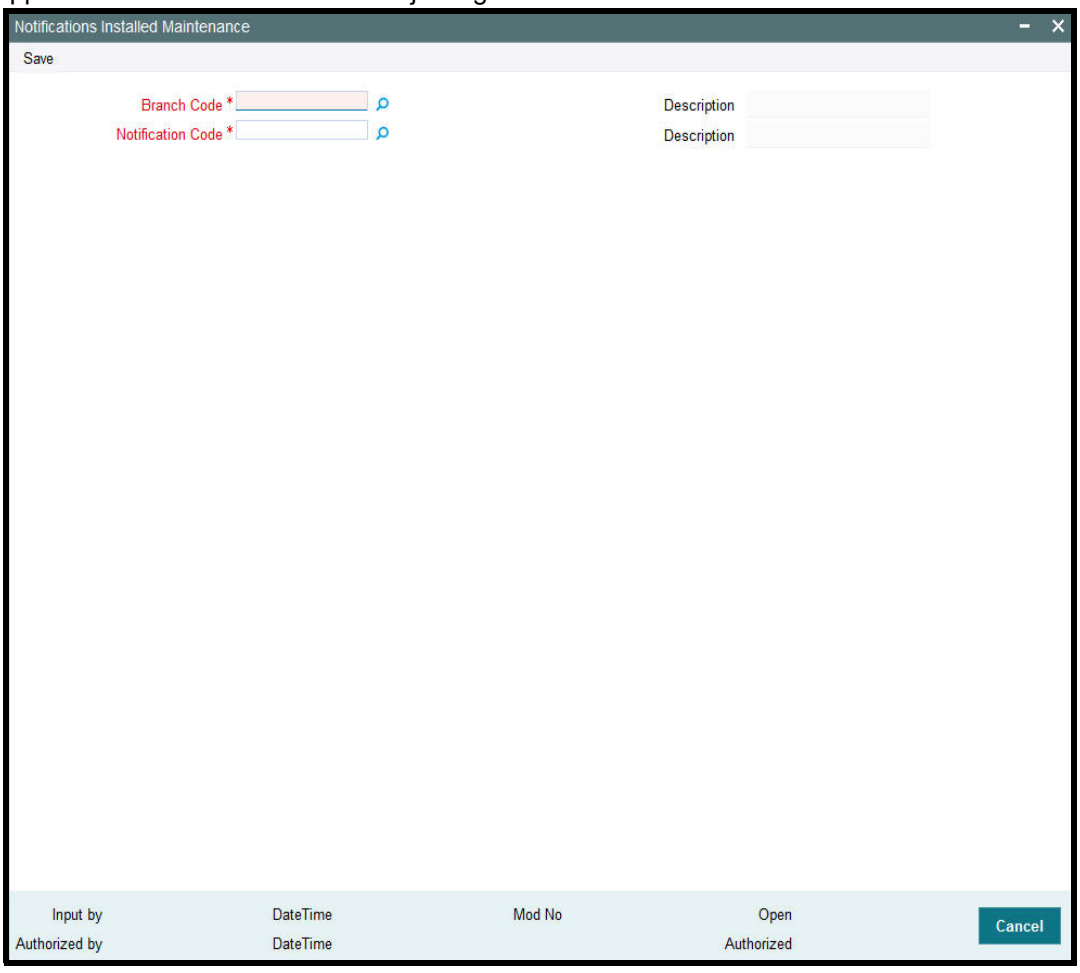
4.19 Notifications Installed Maintenance

This section contains the following topics:

- Section 4.19.1, "Invoking Notifications Installed Maintenance Screen"

4.19.1 Invoking Notifications Installed Maintenance Screen

You can maintain installed notifications using 'Notifications Installed Maintenance' screen. You can invoke this screen by typing 'UTDNTFIN' in the field at the top right corner of the Application tool bar and click the adjoining arrow.



You can specify the following details:

Branch Code

Alphanumeric; 12 Characters; Mandatory

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

Description

Display

The system displays the description for the selected branch code.

Notification Code

Alphanumeric; 120 Characters; Mandatory

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

Description

Display

The system displays the description for the selected notification code.

4.20 PIPA Audit Log

This section contains the following topic:

- Section 4.20.1, "Uploading PIPA Audit Log"

4.20.1 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

Function ID	Description	Audit against the Operations
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
UTDACCLS	UH Status Change -> Detail	New/ Delete/ Authorize/ Query/ Modify
UTDADJ02	Transaction -> Adjustment Subscription	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

Function ID	Description	Audit against the Operations
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
UTDDCTRO	UH Dividend Component Over-ride -> Detail	New/ Delete/ Authorise/ Query/ Modify
UTDFATMT	FATCA -> Entity FATCA Classifi-cation	New/ Delete/ Authorize/ Query/ Modify
UTDFNBAL	Investor fund Balance -> Sum-mary	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 -> Propa-gation 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

Function ID	Description	Audit against the Operations
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
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. Tanking of Maintenance Records

The maintenance records that are created or modified in the system can be tanked till they get authorized, so that it is possible to undo the modifications, if needed, before the records are authorized. The maintenance log also will store the changes till they get authorized. The new or the modified records are written to the static tables only after authorization.

This chapter contains the following sections:

5.1 Tanking New and Modified Maintenance Records

This section contains the following topics:

5.1.1 Enabling Tanking of Maintenance Records

You can enable tanking of the creation and modification of maintenance records by selecting the 'Tanking Required' option provided at the function ID level. You need to enable the 'Tanking Required' option in RAD tool as well.

Tanking of records has been enabled only for the following function IDs:

FUNCTION_ID	MAIN_MENU	SUB_MENU_1	DESCRIPTION
UTDGLACM	A/c System GL Setup	Detail	Accounting System GL Setup Detail
UTDATREP	Auth Rep	Detail	Auth Rep Maintenance Detail
UTDASSSD	AutoSwitch SetUp	Detail	AutoSwitch Setup Detail
UTDBRKTY	Broker Type	Detail	Broker Type Detail
UTDCMPMN	Campaign Mainte-nance	Detail	Campaign Maintenance
UTDCONPF	Country Preference	Detail	Country Preference Main-tenance Detail
UTDCURCT	Currency Cut-Off	Detail	Currency Cut-off Detail

FUNCTION_ID	MAIN_MENU	SUB_MENU_1	DESCRIPTION
UTDENTCO	Entity Comm.Share	Detail	Entity Commission Sharing Detail
UTDBRIDS	Entity IDS	Detail	Income Distribution Setup Detail
UTDVEST	Entity Media Maintenance	Detail	Entity Media Maintenance
UTDFATMT	FATCA	Entity FATCA Classification	Entity FATCA Classification Maintenance Detail
UTDFATDT	FATCA	FATCA Document Maintenance	FATCA Document Maintenance Detail
UTDFAR	FBC Accs Restriction	Detail	FBC Access Restriction Detail
UTDFRQPR	Freq Preference	Detail	Frequency Preferences Detail
UTDFNDAC	Fund Account	Detail	Fund Account Input Detail
UTDFALMT	Fund Agency Limit	Detail	Fund Agency BackDating Limit Setup Detail
UTDFNENT	Fund Entity	Detail	Fund Entity Mapping Detail
UTDFNDFM	Fund Family	Detail	Fund Family Detail
UTDFPHOL	Fund Price Holiday	Detail	Fund Price Holiday Maintenance Detail
UTDFNDRL	Fund Rules	Fund Rules	Fund Rules Detail
UTDFSAMS	Fund Sub Acc Mapping	Detail	Fund Sub Account Mapping Detail
UTDFNSWR	Fund Switch Restrict	Detail	Fund Switch Restrict Detail
UTDFNDUS	Fund User	Fund User	Fund User Restriction
UTDFNDIS	Fund-ISIN Mapping	Detail	Fund-ISIN Mapping Detail
UTDGFPLR	GF Policy Restrict Mapping	Detail	GF Policy Restrict Mapping
UTDGLISD	GL Interface Set-Up	Detail	GL Interface Set-Up Detail
UTDGRPCH	Group Character	Detail	Group Characteristics Detail
UTDHWM	High Water Mark Maintenance	Detail	High Water Mark Maintenance

FUNCTION_ID	MAIN_MENU	SUB_MENU_1	DESCRIPTION
UTDHOLID	Holiday Maintenance	Detail	Holiday Maintenance Detail
UTDKYCMT	KYC Maintenance	Detail	KYC Maintenance Detail
LEDCMSD	LEP Maintenance	Cession	Cession Maintenance Detail
LEDMGMAP	LEP Maintenance	Management Fee	Management Fee Applicability Detail
LEDPROD	LEP Maintenance	Product	Product Maintenance Detail
LEDPRBON	LEP Maintenance	Product Bonus	Product Bonus Maintenance Detail
LEDPRDEN	LEP Maintenance	Product Entity Maintenance	Product Entity Maintenance Detail
LEDPNFM	LEP Maintenance	Product Nature Of Fund Mapping	Product Nature Of Fund Mapping
LEDPRTAX	LEP Maintenance	Product Tax Class Maintenance	Product Tax Class Maintenance Detail
LEDPRSUB	LEP Maintenance	Product Transaction Sub Type Mapping	Product Transaction Sub Type Mapping Detail
LEDPRTYP	LEP Maintenance	Product Type	Product Type Maintenance Detail
LEDPWHTD	LEP Maintenance	Product WHT Setup	Product With-holding Tax Detail
LEDPAALM	LEP Maintenance	Product-Annual Annuity Limit Mapping	Product Annual Annuity Limit Detail
UTDPAYGP	Payment Group Maintenance	Detail	Payment Group Maintenance
UTDRSPM	Plan Maintenance	Detail	Plan Maintenance Detail
SMDPRTMN	Printer maintenance	Detail	Printer maintenance
UTDSWLAG	Pseudo Switch Lag	Detail	Pseudo Switch Lag Maintenance
UTDENTRL	Relationship Maint	Detail	Relationship Maintenance Detail
UTDSCDEF	Share Class	Detail	Share Class Definition Detail

FUNCTION_ID	MAIN_MENU	SUB_MENU_1	DESCRIPTION
UTDSUBFN	Sub Fund Share Class	Detail	Sub Fund Share Class Detail
UTDSWMSG	Swift Message Setup	Detail	Swift Message Setup Maintenance Detail
UTDSWPRV	Switch Privilege	Detail	Switch Privilege Setup Detail
UTDMINHL	UH Category Holding Period	Detail	Fund UH Category Minimum Holding Period Detail
UTDUHIDS	UH IDS Setup	Detail	Income Distribution Setup Detail
UTDUHIOF	UH IRRF Preference	Detail	Unit Holder IRRF Preference Detail
UTDUHLOI	UH LOI	Detail	Unit Holder LOI Setup Detail
UTDUHNPI	UH NPI Preference	Detail	Unit Holder NPI Preference Detail
UTDUHCOE	Unit Holder Currency of Expression	Detail	Unit Holder Currency of Expression
UTDUH	Unitholder	Detail	Unit Holder Maintenance Detail

5.1.2 Tanking New Records

During the creation of a new record, if 'Tanking Required' option is enabled, the system tanks the details of the newly created record till the record gets authorized. Any query on this data retrieves this stored information.

5.1.3 Tanking Modified Records

All modifications to unauthorized records get tanked and the modified data gets written to actual tables only after authorization. In this case, the record remains in 'Authorized' status in the actual table and the unauthorized modifications will be kept pending for un-tanking. The most recent modifications will be shown in both summary and detailed screens with the Authorization status as 'Unauthorized'.

Note

Reject of tanked unitholder modifications are supported for unit holder that are authorized at least once. You can use 'Delete' to remove modifications prior to authorization.

5.1.4 Closing a Record

You can close a record only if it is in 'Authorized' state, without any unauthorized modifications pending for un-tanking. Closure is possible only for records that are in 'Open' status. When

you close a record, the system tanks this and the record gets actually closed only after the closure gets authorized.

5.1.5 Re-opening a Record

You can re-open a record only if it has been closed and the closure is authorized. Re-opening of a record gets tanked till it gets authorized and the actual re-opening happens after the authorization.

5.1.6 Authorizing a Record

All unauthorized modifications get displayed when you click ‘Authorize’ menu option. You can select a modification number and the records get authorized till that modification. These records are un-tanked and their status gets updated as ‘Authorized’. You can authorize the modifications partially, if required.

5.1.7 Deleting a Record

All unauthorized records will be available for deletion. You can select a modification number and system deletes all unauthorized modifications from the selected modification number. If the modifications getting deleted are made by a user other than the current user, the system displays an error message.

5.1.8 Viewing Summary of Records

All summary screens display data retrieved from both the summary data source and the table that contains the unauthorized tanked records.

5.1.9 Modifying Tanking Preferences

You can modify the tanking preferences specified for a function ID, if required. This modification is possible only if all records related to that function Id are in ‘Authorized’ status.

6. Function ID Glossary