Oracle® FLEXCUBE Investor Servicing
Security User Guide

Release 14.7.6.0.0

G30486-01

April 2025

ORACLE®

Oracle FLEXCUBE Investor Servicing Security User Guide, Release 14.7.6.0.0

G30486-01

Contents

2   Enable Auto Authorization

3   External System Maintenance

ORACLE

4   Tanking of Maintenance Records

Index

Preface

Oracle FLEXCUBE Investor Servicing is a comprehensive mutual funds automation software from Oracle® Financial Servicing Software Ltd.©.

You can use the system to achieve optimum automation of all your mutual fund investor servicing processes, as it provides guidelines for specific tasks, descriptions of various features and processes, and general information.

This topic contains the following sub-topics:

- Purpose
- Audience
- Documentation Accessibility
- Critical Patches
- Diversity and Inclusion
- Conventions
- Screenshot Disclaimer
- Acronyms and Abbreviations
- Symbols and Icons
- Basic Actions
- Getting Help
- Prerequisite

Purpose

You are intended to become familiar with the **Oracle Flexcube Investor Servicing** application through this guide. This guide offers responses to particular features and procedures that are necessary for the module to operate effectively.

Audience

This user guide is intended for the Fund Administrator users and System operators in the AMC.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

Acronyms and Abbreviations

The list of the acronyms and abbreviations used are as follows:

Table   Acronyms and Abbreviations

Abbreviation	Description
CIF	Customer Information File
EOD	End of Day
EPU	Earnings per unit
FCIS	Oracle FLEXCUBE Investor Servicing

ORACLE®

Table   (Cont.) Acronyms and Abbreviations

Abbreviation	Description
FMG	The Fund Manager component of the system
FPADMIN	Oracle FLEXCUBE Administrator
GTA	Global Transfer Agency
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

Symbols and Icons

This guide may refer to all or some of the following symbols and icons:

Table   Symbols and Icons
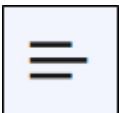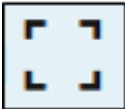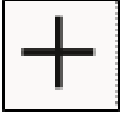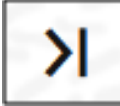
Symbol/Icon	Function
	Lists all records maintained
	Minimize
	Maximize
	Close
	Perform Search

Table   (Cont.) Symbols and Icons

Symbol/Icon	Function
▼	Open a list
📅	Select a Date
✛	Add a new row to enter details in a record.
▬	Delete a row, which is already added.
|◀	Navigate to the first record
▶|	Navigate to the last record
◀	Navigate to the previous record
▶	Navigate to the next record
▤	View a single record
⌄⌃	Sort the values in ascending or descending order
⌄	Sort the values in ascending
⌃	Sort the values in ascending

Basic Actions

Following are the basic actions of the screens that an user may require to perform on new or existing records in a screen.

Table   Basic Actions

Action	Description
New	Used to add a new record. When the user click **New**, the system displays a new record enabling to specify the required data. **Note**: The fields, which are marked with an asterisk, are mandatory.
Copy	Used to copy the details of a record.
Close	Used to close a record. This action is available only when a record is created.
Unlock	Used to update the details of an existing record. System displays an existing record in editable mode.
Print	Used to print a record. This action is available only when a record is created.
Enter Query	Used to give details of a saved record in a detail screen. When the user click **Enter Query**, the system displays a saved record enabling to specify only the required or primary data.
Execute Query	User need to perform this after entering query. Click **Execute Query** after specifying the details of the record to be fetched, the system retrieves all the information of that particular record.
Audit	Used to view the maker details, checker details and report status.
Cancel	Used to cancel the performed action.
Save	Used to save the details entered or selected in the screen.
Refresh	Used to refresh the details selected in the screen.
Reset	Used to reset the fields to enter a new criteria.
Clear All	Used to clear all the data entered for search criteria.
Details	Used to navigate to Detail screen.
Search	Used to search either the details of a particular record or a list of records by querying particular field.
Advanced Search	Used to search details more precisely.
Approve	Used to approve the initiated report. This button is displayed, once the user click **Authorize**.
Authorize	Used to authorize the report created. A maker of the screen is not allowed to authorize the report. Only a checker can authorize a report, created by a maker.
Confirm	Used to confirm the performed action.
OK	Used to confirm the details in the screen.
Reject	Used to reject the report created. A maker of the screen is not allowed to authorize the report. Only a checker can reject a report, created by a maker.

ORACLE®

Table   (Cont.) Basic Actions

Action	Description
View	Used to view the report details in a particular modification stage. This button is displayed, once the user click **Authorize**.

Getting Help

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

Prerequisite

Specify **User ID** and **Password**, and log in to **Home Screen**.

1
Ensure Security for Fund Manager

This topic takes you through the Security Maintenance features of the **Oracle FLEXCUBE Investor Servicing** system.

In any financial environment, security of information is of paramount importance. Access to information must be made available in a carefully monitored manner. The 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.

You will learn how to use the security features in the system to suit your requirements and customize them for your environment.

- **Security Management**
  This topic explains about the management of security system.

- **Terms and Definition**
  This topic contains some important terms and their explanations that you will encounter during the process.

- **Other Features of Security Management System**
  This topic explains some other features of Security Management System.

- **Process Role Definition**
  This topic provides the systematic instructions to define Role Profiles.

- **Role Definition Summary**
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- **Process User Admin**
  This topic provides the systematic instructions to define User Profiles.

- **User Admin Summary**
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- **Process Hot Keys Maintenance**
  This topic provides the systematic instructions to set the most used screens in hot keys and launch the same using the hot key combination.

- **Process SMS Parameters Maintenance**
  This topic provides the systematic instructions to set up certain parameters related to invalid logins and passwords.

- **Process User Credentials Change**
  This topic provides the systematic instructions to change or reset user passwords in bulk.

- **User Credentials Change Summary**
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- **Set up Modules**
  This topic provides information on setting up modules.

- Process Printer Maintenance
  This topic provides the systematic instructions to process printer maintenance.

- Printer Maintenance Summary
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- Process Row Level Security Maintenance
  This topic provides the systematic instructions to enable or disable Row Level Security (RLS) policy.

1.1 Security Management

This topic explains about the management of security system.

In **Oracle FLEXCUBE Investor Servicing**, 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

1.2 Terms and Definition

This topic contains some important terms and their explanations that you will encounter during the process.

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

Table 1-1   Terms and Definition

Terms	Definition
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.

Table 1-1 (Cont.) Terms and Definition

Terms	Definition
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 Investor Servicing** 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.

1.3 Other Features of Security Management System

This topic explains some other features of Security Management System.

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

Table 1-2 Features and Explanation

Features	Explanation
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.
Restricted Access to Branches	You can indicate the branches from where a user can operate.
	Click the **User Branch Restrictions** button in the **User Profile Definition** screen to define the branches from where a user can operate.

Table 1-2   (Cont.) Features and Explanation

Features	Explanation
Restricted Access to AMC Branches	You can indicate the branches of the AMC from where a user can operate for mutual fund account customers.
	Click 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.
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.

1.4 Process Role Definition

This topic provides the systematic instructions to define Role Profiles.

1. On **Home** screen, type **SMDROLDF** in the text box, and click **Next**.

    The **Role Definition** screen is displayed.

Figure 1-1   Role Definition

2. On **Role Definition** screen, click **New** to enter the details.

    For more information on fields, refer to the field description table.

Table 1-3   Process Role Definition - Field Description

Field	Description
Role Identification	*Alphanumeric, 15 Characters; Mandatory*
	Specify a unique identifier for the role profile.

Table 1-3   (Cont.) Process Role Definition - Field Description

Field	Description
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	You should define the functions to which the role profile has access after you have defined the basic attributes of a Role Profile (the Role ID, Description, Module and whether it is Customer- Specific) in this section. 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 Functions	*Alphanumeric; 8 Characters; Mandatory* Select the function that you want to link to the role profile.

3. You can allow or disallow specific record-level operations for each function.

   The operations **New**, **Copy**, **Delete**, **Close**, **Unlock**, **Reopen**, **Print**, **Auth**, **Reverse** are displayed as a horizontal list, alongside the Maintenance Functions label.

4. Check the box pertaining to each operation you want to allow for the role profile in the selected function row.

Classify Role Profile

5. You define a Role Profile for the users who are employees of your AMC or AMC branch.

6. You can indicate that the profile is for customers who might log in from remote terminals to inquire on their transactions and balances using **Customer Specific** field.

• Static Tables
  This topic provides the systematic instructions to allow the various operations at record level for the role profile.

• Contracts and Online Transaction Processing
  This topic provides information on Contracts and Online Transaction Processing.

• Reports
  This topic provides information on Reports generation.

1.4.1 Static Tables

This topic provides the systematic instructions to allow the various operations at record level for the role profile.

1. On **Role Definition** screen, you can define the functions to which the role profile has access.

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

   The following operations are listed:

   - **New** - To define a new record
   - **Copy** - To copy details of an existing record
   - **Delete** - To delete an existing record
   - **Close** - To close an existing record
   - **Unlock** - To amend an existing record
   - **Reopen** - To reopen an existing record
   - **Print** - To print the details of selected records
   - **Authorize** - To authorize any maintenance activity on a record
   - **Reverse** - To reverse the details of selected records

1.4.2 Contracts and Online Transaction Processing

This topic provides information on Contracts and Online Transaction Processing.

View (to see the details of the contract).

1.4.3 Reports

This topic provides information on Reports generation.

You can do any of the following:

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

1.5 Role Definition Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve Role Definition Record

1. On **Home** screen, type **SMSROLDF** in the text box, and click **Next**.

   The **Role Definition Summary** screen is displayed.

Figure 1-2   Role Definition Summary

2. On **Role Definition Summary** screen, specify any or all of the following details in the corresponding fields:

    •   **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

    •   **Record Status**

    •   **Role Identification**

    •   **Description**

3. Click **Search** button to view the records.

    All the records with the specified details are retrieved and displayed in 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 **Role Identification**

    •   Press F8

    ---

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

•   Edit Role Definition Record
    This topic provides the systematic instructions to edit Role Definition record.

•   View Role Definition Record
    This topic provides the systematic instructions to view Role Definition record.

•   Delete Role Definition Record
    This topic provides the systematic instructions to delete Role Definition record.

•   Authorize Role Definition Record
    This topic provides the systematic instructions to authorize Role Definition record.

- Amend Role Definition Record
  This topic provides the systematic instructions to amend Role Definition record.
- Authorize Amended Role Definition Record
  This topic provides the systematic instructions to authorize amended Role Definition record.
- Copy Role Definition Record
  This topic provides the systematic instructions to copy Role Definition record.

1.5.1 Edit Role Definition Record

This topic provides the systematic instructions to edit Role Definition record.

Modify the details of Role Definition Record that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **Role Definition Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

    All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

    The **Role Definition** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. Click **Save** to save your changes.

    The **Role Definition** screen is closed and the changes made are reflected in the **Role Definition Summary** screen.

1.5.2 View Role Definition Record

This topic provides the systematic instructions to view Role Definition record.

View a record that you have previously input by retrieving the same in the **Role Definition Summary** screen. Perform this operation as follows:

1. Start the **Role Definition Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

    All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **Role Definition** screen is displayed.

1.5.3 Delete Role Definition Record

This topic provides the systematic instructions to delete Role Definition record.

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

1. Start the **Role Definition Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **Role Definition** screen is displayed.

5. 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.

1.5.4 Authorize Role Definition Record

This topic provides the systematic instructions to authorize Role Definition record.

Authorize an unauthorized Role Definition Record in the system for it to be processed as follows:

1. Start the **Role Definition Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **Role Definition** screen is displayed.

5. 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.

1.5.5 Amend Role Definition Record

This topic provides the systematic instructions to amend Role Definition record.

Modify the details of an authorized record using the **Unlock** operation from the Action List. To make changes to a record after authorization:

1. Start the **Role Definition Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for amendment.

You can only amend authorized records.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details are retrieved and displayed in the screen.

4. Double-click the record that you wish to amend.

   The **Role Definition** screen is displayed.

5. Select **Unlock** operation from the Action List to amend the record.

6. Amend the necessary information and click **Save** to save the changes.

1.5.6 Authorize Amended Role Definition Record

This topic provides the systematic instructions to authorize amended Role Definition record.

Authorize an amended Role Definition Record 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 process of subsequent authorization is the same as that for normal transactions.

1.5.7 Copy Role Definition Record

This topic provides the systematic instructions to copy Role Definition record.

1. Click **Copy** to create a new **Role Definition** with the same attributes of an existing record.

2. Retrieve the record whose attributes the new **Role Definition** should inherit.

   You can retrieve the record through the Summary screen or through the F7-F8 operation explained in the previous steps.

3. Click **Copy**.

   Indicate the ID for the new **Role Definition**. You can, however, change the details of the new record.

1.6 Process User Admin

This topic provides the systematic instructions to define User Profiles.

1. On **Home** screen, type **SMDUSRDF** in the text box, and click **Next**.

   The **User Admin** screen is displayed.

Figure 1-3   User Admin

2. On **User Admin** screen, click **New** to enter the details.

    For more information on fields, refer to the field description table.

Table 1-4   User Admin - Field Description

Field	Description
User Details	The section displays the following fields.
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 **Oracle FLEXCUBE Investor Servicing** is mapped to the subject (DN) while authentication via SSO. Four SSO types **SAML**, **TOKEN, IDCS_TOKEN** and **DEFAULT** are currently supported in FCIS. Refer to the topic *FCIS_Property_File_Creation* for setting up FCIS to support SSO.
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.

Table 1-4   (Cont.) User Admin - Field Description

Field	Description
Language	*Alphanumeric; 3 Characters; Mandatory* Specify the preferred language for the user profile. Alternatively, you can also select language from the option list. The list displays all valid language code maintained in the system.
Home Branch	*Alphanumeric; 3 Characters; Mandatory* Specify the home branch details.
Home Module	*Alphanumeric; 30 Characters; Mandatory* Specify the default module from which the user profile will operate.
Debug Window Enabled	*Optional* Check this box to enable debug window.
Show Dashboard	*Optional* Check this box to show dashboard.
Classification	*Optional* Select one of the classification options: • **Staff** • **Auto End Of Day** • **Customer** You can classify a user as belonging to one of the following categories: • **Staff:** A user of the system who is an employee of your 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 Admin** 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 (PII)** has to be viewed or not from the drop-down list. The list displays the following values: • **Yes** • **No** **View PII** field is set to **Yes** by default. 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.

Table 1-4   (Cont.) User Admin - Field Description

Field	Description
Modules	The section displays the following fields.
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	The section displays the following fields.
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	The section displays the following fields.
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	The section displays the following fields.

Table 1-4   (Cont.) User Admin - Field Description

Field	Description
Password	*Alphanumeric; 32 Characters; Optional* Specify the user password to log in. 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 preset 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	The section displays the following fields.
Limit Currency	*Alphanumeric; 3 Characters; Mandatory* Specify the currency to be mapped for transaction amount and auth amount.

Table 1-4   (Cont.) User Admin - Field Description

Field	Description
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**

• **Restrictive Passwords**
  This topic provides the systematic instructions to maintain a list of passwords that the user must not use.

• **Module Button**
  This topic provides the systematic instructions to restrict the user to operate only from certain modules.

• **Roles Button**
  This topic provides the systematic instructions to define a role to the user profile.

• **Functions Button**
  This topic provides the systematic instructions to give access to functions for the user profiles.

• **Branches Button**
  This topic provides the systematic instructions to define the branches to operate.

ORACLE

- **Disallowed Functions Button**
  This topic provides the systematic instructions to define a list of functions that the user is not allowed to operate.

- **Dashboard Mapping Button**
  This topic provides the systematic instructions to map the dashboards.

- **Other Attributes for User Profile**
  This topic explains the other attributes for a User Profile.

- **Static Tables**
  This topic provides the systematic instructions to allow the various operations at record level for the role profile.

- **Contracts and Online Transaction Processing**
  This topic provides information on Contracts and Online Transaction Processing.

- **Reports**
  This topic provides information on Reports generation.

1.6.1 Restrictive Passwords

This topic provides the systematic instructions to maintain a list of passwords that the user must not use.

1. On **User Admin** screen, click **Restrictive Passwords** button to enter the details.

   The **Restrictive Passwords** screen is displayed.

   Figure 1-4   User Admin_Restrictive Passwords Button

2. 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.

3. On **Restrictive Passwords** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-5   Restrictive Passwords - Field Description

Field	Field Description
Password	*Alphanumeric; 12 Characters; Mandatory* Specify the restricted password. **Note:** The user for whom you are defining the restrictive passwords cannot use the restrictive passwords defined in this screen.

1.6.2 Module Button

This topic provides the systematic instructions to restrict the user to operate only from certain modules.

1. On **User Admin** screen, click **Module** button to define a restrictive list of AMC's or AMC branches.

   The **Module** screen is displayed.

Figure 1-5   User Admin_Module Button

2. You can restrict the user to operate only from certain modules, or branches of an AMC.

3. On **Module** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-6   Module - Field Description

Field	Field Description
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.

1.6.3 Roles Button

This topic provides the systematic instructions to define a role to the user profile.

1. On **User Admin** screen, click **Roles** button to attach the user profile you are defining to a role.

   The **Roles** screen is displayed.

Figure 1-6   User Admin_Roles Button

2. On **Roles** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-7   Roles - Field Description

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

3. Click **Save** to save your changes when you have selected the required roles.

1.6.4 Functions Button

This topic provides the systematic instructions to give access to functions for the user profiles.

1. On **User Admin** screen, click **Functions** button to give access to functions for the user profile you are defining.

   The **Functions** screen is displayed.

Figure 1-7   User Admin_Functions Button

2. You can give access to specific functions for a user profile to which no role is 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.

   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.

3. On **Functions** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-8   Functions - Field Description

Field	Field Description
Function	*Alphanumeric; 3 Characters; Mandatory* Specify the function id from the option list.
Module ID	*Alphanumeric; 30 Characters; Mandatory* Specify the module ID from the option list.

1.6.5 Branches Button

This topic provides the systematic instructions to define the branches to operate.

1. On **User Admin** screen, click **Branches** button to define the branches in which the user should be allowed to operate.

   The **Branches** screen is displayed.

Figure 1-8   User Admin_Branches Button

2. You can specify the branches from which they can operate for Staff and End of Day users.

3. On **Branches** screen, specify the fields.

   For more information on fields, refer to the field description table.

Table 1-9   Branches - Field Description

Field	Field Description
Branches	*Optional* Select one of the options from the following list: • **Allowed** • **Disallowed** Choose **Disallowed** option to prepare a list of branches from which the user is disallowed. Specify the branches that are disallowed for a user. Similarly, choose **Allowed** option to prepare a list of branches from which the user is allowed to operate.
Branch List	The section displays the following fields.
Branch	*Alphanumeric; 30 Characters; Mandatory* Specify the branch code.
Branch Name	*Display* The system displays the name of the branch for the selected branch code.

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.

Table 1-10   Allow User to Operate from Different Branches

Users	Functions
Allow 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.
User Transaction and Auth Limits	You cannot capture any transaction, if the transaction amount is greater than the maximum transaction amount. Also, you cannot authorize 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.

1.6.6 Disallowed Functions Button

This topic provides the systematic instructions to define a list of functions that the user is not allowed to operate.

1. On **User Admin** screen, click **Disallowed Functions** button to define a list of functions that the user is not allowed to operate, out of the functions list already associated with the user profile.

All the functions that are associated with the user profile are listed in the Available box.

The **Disallowed Functions** screen is displayed.

Figure 1-9   User Admin_Disallowed Functions Button

2. On **Disallowed Functions** screen, specify the fields.

   For more information on fields, refer to the field description table.

   Table 1-11   Disallowed Functions - Field Description

Field	Field Description
Function	*Alphanumeric; 8 Characters; Mandatory* Specify the function id from the option list.
Module ID	*Alphanumeric; 30 Characters; Mandatory* Specify the module ID from the option list.

1.6.7 Dashboard Mapping Button

This topic provides the systematic instructions to map the dashboards.

1. On **User Admin** screen, click **Dashboard Mapping** button to map the dashboards.

   The **Dashboard Maintenance** screen is displayed.

Figure 1-10   Dashboard Maintenance

2. On **Dashboard Maintenance** screen, specify the fields.

   For more information on fields, refer to the field description table.

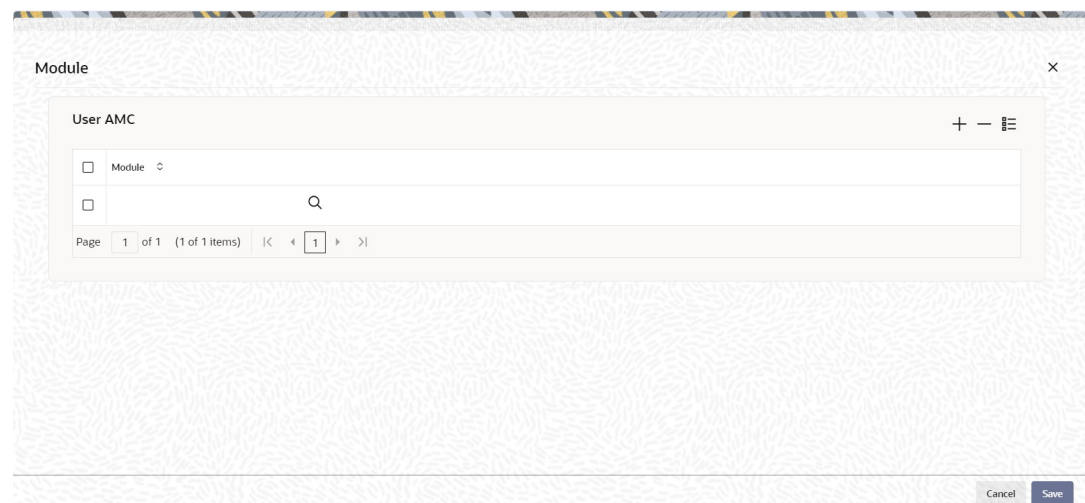   **Table 1-12   Dashboard Maintenance - Field Description**

Field	Field Description
User ID	*Display* The system displays the user ID.
User Name	*Display* The system displays the user name for the selected user ID.

3. Click the **Populate** button.

   The system displays the following details:

   • **Function**

   • **Description**

   • **Sequence Number**

   • **Clause Wizard** Button

   • **Where Clause**

   • **Show In Dashboard** Button

• Clause Wizard Button
  This topic provides the systematic instructions to process the dashboard condition.

1.6.7.1 Clause Wizard Button

This topic provides the systematic instructions to process the dashboard condition.

1. On **Dashboard Maintenance** screen, click the **Clause Wizard** button.

   The **Dashboard Condition** screen is displayed.

Figure 1-11   Dashboard Condition

2. On **Dashboard Condition** screen, specify the fields.

    For more information on fields, refer to the field description table.

    Table 1-13   Dashboard Condition - Field Description

Field	Field Description
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.

1.6.8 Other Attributes for User Profile

This topic explains the other attributes for a User Profile.

You can define any of the following attributes other than the attributes you have defined for a user profile, such as the role association, function access rights, restrictive passwords, and branch restrictions. 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.

1.6.9 Static Tables

This topic provides the systematic instructions to allow the various operations at record level for the role profile.

1. On **Role Definition** screen, you can define the functions to which the role profile has access.
2. You can allow any of the following operations at record level for the role profile in any function.

   The following operations are listed:

   - **New** - To define a new record
   - **Copy** - To copy details of an existing record
   - **Delete** - To delete an existing record
   - **Close** - To close an existing record
   - **Unlock** - To amend an existing record
   - **Reopen** - To reopen an existing record
   - **Print** - To print the details of selected records
   - **Authorize** - To authorize any maintenance activity on a record
   - **Reverse** - To reverse the details of selected records

1.6.10 Contracts and Online Transaction Processing

This topic provides information on Contracts and Online Transaction Processing.

View (to see the details of the contract).

1.6.11 Reports

This topic provides information on Reports generation.

You can do any of the following:

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

1.7 User Admin Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve User Admin Record

1. On **Home** screen, type **SMSUSRDF** in the text box, and click **Next**.

   The **User Admin Summary** screen is displayed.

Figure 1-12   User Admin Summary

2. On **User Admin Summary** screen, specify any or all of the following details in the corresponding fields:

   - **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   - **Record Status**

   - **User Identification**

   - **Name**

   - **Home Branch**

   - **Start Date**

   - **Classification**

3. Click **Search** button to view the records.

   All the records with the specified details are retrieved and displayed in 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

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

- Edit User Admin Record
  This topic provides the systematic instructions to edit User Admin record.

- View User Admin Record
  This topic provides the systematic instructions to view User Admin record.

- Delete User Admin Record
  This topic provides the systematic instructions to delete User Admin record.

- Authorize User Admin Record
  This topic provides the systematic instructions to authorize User Admin record.

- Amend User Admin Record
  This topic provides the systematic instructions to amend User Admin record.

- Authorize Amended User Admin Record
  This topic provides the systematic instructions to authorize amended User Admin record.

- Copy User Admin Record
  This topic provides the systematic instructions to copy User Admin record.

1.7.1 Edit User Admin Record

This topic provides the systematic instructions to edit User Admin record.

Modify the details of User Admin Record that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **User Admin Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

   All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

   The **User Admin** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. Click **Save** to save your changes.

   The **User Admin** screen is closed and the changes made are reflected in the **User Admin Summary** screen.

1.7.2 View User Admin Record

This topic provides the systematic instructions to view User Admin record.

View a record that you have previously input by retrieving the same in the **User Admin Summary** screen. Perform this operation as follows:

1. Start the **User Admin Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **User Admin** screen is displayed.

1.7.3 Delete User Admin Record

This topic provides the systematic instructions to delete User Admin record.

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

1. Start the **User Admin Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **User Admin** screen is displayed.

5. 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.

1.7.4 Authorize User Admin Record

This topic provides the systematic instructions to authorize User Admin record.

Authorize an unauthorized User Admin Record in the system for it to be processed as follows:

1. Start the **User Admin Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **User Admin** screen is displayed.

5. 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.

1.7.5 Amend User Admin Record

This topic provides the systematic instructions to amend User Admin record.

Modify the details of an authorized record using the **Unlock** operation from the Action List. To make changes to a record after authorization:

1. Start the **User Admin Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for amendment.

   You can only amend authorized records.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details are retrieved and displayed in the screen.

4. Double-click the record that you wish to amend.

   The **User Admin** screen is displayed.

5. Select **Unlock** operation from the Action List to amend the record.

6. Amend the necessary information and click **Save** to save the changes.

1.7.6 Authorize Amended User Admin Record

This topic provides the systematic instructions to authorize amended User Admin record.

Authorize an amended User Admin Record 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 process of subsequent authorization is the same as that for normal transactions.

1.7.7 Copy User Admin Record

This topic provides the systematic instructions to copy User Admin record.

1. Click **Copy** to create a new User Admin with the same attributes of an existing record.

2. Retrieve the record whose attributes the new User Admin should inherit.

   You can retrieve the record through the Summary screen or through the F7-F8 operation explained in the previous steps.

3. Click **Copy**.

   Indicate the ID for the new User Definition. You can, however, change the details of the new record.

1.8 Process Hot Keys Maintenance

This topic provides the systematic instructions to 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 IDs 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.

1. On **Home** screen, type **SMDHOTKY/ UTDHOTKY** in the text box, and click **Next**.

   The **Hot Keys Maintenance** screen is displayed.

Figure 1-13   Hot Keys Maintenance

2. On **Hot Keys Maintenance** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 1-14   Hot Keys Maintenance - Field Description

Field	Description
User ID	*Display* The system displays the logged in user ID.
Hot Key	The section displays the following fields.
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.

Table 1-14   (Cont.) Hot Keys Maintenance - Field Description

Field	Description
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.

1.9 Process SMS Parameters Maintenance

This topic provides the systematic instructions to set up certain parameters related to invalid logins and passwords.

1. On **Home** screen, type **SMDPARAM** in the text box, and click **Next**.

   The **SMS Parameters Maintenance** screen is displayed.

Figure 1-14   SMS Parameters Maintenance

2. On **SMS Parameters Maintenance** screen, click **Enter Query** to display the SMS parameters.

    For more information on fields, refer to the field description table.

Table 1-15   SMS Parameters Maintenance - Field Description

Field	Description
Password Length (Characters)	The section displays the following fields.
Maximum	*Numeric; 2 Characters; Optional* Specify 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* Specify 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	The section displays the following fields.
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.

Table 1-15   (Cont.) SMS Parameters Maintenance - Field Description

Field	Description
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	The section displays the following fields.
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.

Table 1-15   (Cont.) SMS Parameters Maintenance - Field Description

Field	Description
Minimum Number of Numeric Characters in Password	*Numeric; 2 Characters; Optional* Define the minimum number of numeric characters that are 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 that are 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 that are 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	The section displays the following fields.
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 screensaver interval.
Restricted Passwords	The section displays the following fields.
Restricted Passwords	*Alphanumeric; 12 Characters; Optional* Specify the restricted password.

ORACLE®

1.10 Process User Credentials Change

This topic provides the systematic instructions to change or reset user passwords 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.

1. On **Home** screen, type **SMDCHPWD** in the text box, and click **Next**.

   The **User Credentials Change** screen is displayed.

   Figure 1-15   User Credentials Change

2. On **User Credentials Change** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

   Table 1-16   User Credentials Change - Field Description

Field	Description
Sequence Number	*Display* Click **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.

Table 1-16   (Cont.) User Credentials Change - Field Description

Field	Description
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.

1.11 User Credentials Change Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve User Credentials Change Record

1. On **Home** screen, type **SMSCHPWD** in the text box, and click **Next**.

   The **User Credentials Change Summary** screen is displayed.

Figure 1-16   User Credentials Change Summary

2. On **User Credentials Change Summary** screen, specify any or all of the following details in the corresponding fields:

   • **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   • **Record Status**

   • **Sequence Number**

   • **Description**

   • **Process Date**

3. Click **Search** button to view the records.

   All the records with the specified details are retrieved and displayed in 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

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

   • Edit User Credentials Change Record
     This topic provides the systematic instructions to edit User Credentials Change record.

   • View User Credentials Change Record
     This topic provides the systematic instructions to view User Credentials Change record.

   • Delete User Credentials Change Record
     This topic provides the systematic instructions to delete User Credentials Change record.

   • Authorize User Credentials Change Record
     This topic provides the systematic instructions to authorize User Credentials Change record.

   • Amend User Credentials Change Record
     This topic provides the systematic instructions to amend User Credentials Change record.

   • Authorize Amended User Credentials Change Record
     This topic provides the systematic instructions to authorize amended User Credentials Change record.

1.11.1 Edit User Credentials Change Record

This topic provides the systematic instructions to edit User Credentials Change record.

Modify the details of User Credentials Change Record that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **User Credentials Change Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

   All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

    The **User Credentials Change** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. Click **Save** to save your changes.

    The **User Credentials Change** screen is closed and the changes made are reflected in the **User Credentials Change Summary** screen.

1.11.2 View User Credentials Change Record

This topic provides the systematic instructions to view User Credentials Change record.

View a record that you have previously input by retrieving the same in the **User Credentials Change Summary** screen. Perform this operation as follows:

1. Start the **User Credentials Change Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

    All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

    The **User Credentials Change** screen is displayed.

1.11.3 Delete User Credentials Change Record

This topic provides the systematic instructions to delete User Credentials Change record.

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

1. Start the **User Credentials Change Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

    All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

    The **User Credentials Change** screen is displayed.

5. 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.

1.11.4 Authorize User Credentials Change Record

This topic provides the systematic instructions to authorize User Credentials Change record.

Authorize an unauthorized User Credentials Change Record in the system for it to be processed as follows:

1. Start the **User Credentials Change Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **User Credentials Change** screen is displayed.

5. 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.

1.11.5 Amend User Credentials Change Record

This topic provides the systematic instructions to amend User Credentials Change record.

Modify the details of an authorized record using the **Unlock** operation from the Action List. To make changes to a record after authorization:

1. Start the **User Credentials Change Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for amendment.

   You can only amend authorized records.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details are retrieved and displayed in the screen.

4. Double-click the record that you wish to amend.

   The **User Credentials Change** screen is displayed.

5. Select **Unlock** operation from the Action List to amend the record.

6. Amend the necessary information and click **Save** to save the changes.

1.11.6 Authorize Amended User Credentials Change Record

This topic provides the systematic instructions to authorize amended User Credentials Change record.

Authorize an amended User Credentials Change Record 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 process of subsequent authorization is the same as that for normal transactions.

1.12 Set up Modules

This topic provides information on 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.

• Process Module Setup
This topic provides the systematic instructions to create new agency branch modules.

• Operations on Module Record
This topic gives information on operations on Module Record.

1.12.1 Process Module Setup

This topic provides the systematic instructions to create new agency branch modules.

1. On **Home** screen, type **SMDMODUL** in the text box, and click **Next**.

   The **Module Setup** screen is displayed.

Figure 1-17   Module Setup

Figure 1-18   Policy SI Summary

2. On **Module Setup** screen, click **New** to enter the details.

The System Admin user can create new agency branch modules. For more information on fields, refer to the field description table.

Table 1-17   Module Setup - Field Description

Field	Description
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.

Table 1-17　(Cont.) Module Setup - Field Description

Field	Description
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.

3. Click **Save** to save your user profile record.

The system confirms the saving of the record into the SMS database.

1.12.2 Operations on Module Record

This topic gives information on 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.

Perform the following operations on modules in the **Module Setup** screen.

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

1.13 Process Printer Maintenance

This topic provides the systematic instructions to process printer maintenance.

1. On **Home** screen, type **SMDPRTMN** in the text box, and click **Next**.

   The **Printer Maintenance** screen is displayed.

Figure 1-19   Printer Maintenance

2. On **Printer Maintenance** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 1-18   Printer Maintenance - Field Description

Field	Description
Printer	The section displays the following fields.
Printer ID	*Alphanumeric; 2 Characters; Optional* Specify the printer ID.
Printer Name	*Alphanumeric; 105 Characters; Optional* Specify the printer name.

Table 1-18   (Cont.) Printer Maintenance - Field Description

Field	Description
Branch	*Alphanumeric; 3 Characters; Optional* Specify the branch code.
Roles	The section displays the following fields.
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	The section displays the following fields.
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.

1.14 Printer Maintenance Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve Printer Maintenance Record

1. On **Home** screen, type **SMSPRTMN** in the text box, and click **Next**.

   The **Printer Maintenance Summary** screen is displayed.

Figure 1-20   Printer Maintenance Summary

2. On **Printer Maintenance Summary** screen, specify any or all of the following details in the corresponding fields:

   - **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   - **Record Status**

   - **Printer ID**

- • **Printer Name**
- • **Branch**

3. Click **Search** button to view the records.

   All the records with the specified details are retrieved and displayed in 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 Printer ID/Name
   > - • Press F8

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

- • Edit Printer Maintenance Record
  This topic provides the systematic instructions to edit Printer Maintenance record.

- • View Printer Maintenance Record
  This topic provides the systematic instructions to view Printer Maintenance record.

- • Delete Printer Maintenance Record
  This topic provides the systematic instructions to delete Printer Maintenance record.

- • Authorize Printer Maintenance Record
  This topic provides the systematic instructions to authorize Printer Maintenance record.

- • Amend Printer Maintenance Record
  This topic provides the systematic instructions to amend Printer Maintenance record.

- • Authorize Amended Printer Maintenance Record
  This topic provides the systematic instructions to authorize amended Printer Maintenance record.

1.14.1 Edit Printer Maintenance Record

This topic provides the systematic instructions to edit Printer Maintenance record.

Modify the details of Printer Maintenance Record that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **Printer Maintenance Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

   The **Printer Maintenance** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. Click **Save** to save your changes.

   The **Printer Maintenance** screen is closed and the changes made are reflected in the **Printer Maintenance Summary** screen.

1.14.2 View Printer Maintenance Record

This topic provides the systematic instructions to view Printer Maintenance record.

View a record that you have previously input by retrieving the same in the **Printer Maintenance Summary** screen. Perform this operation as follows:

1. Start the **Printer Maintenance Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **Printer Maintenance** screen is displayed.

1.14.3 Delete Printer Maintenance Record

This topic provides the systematic instructions to delete Printer Maintenance record.

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

1. Start the **Printer Maintenance Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **Printer Maintenance** screen is displayed.

5. 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.

1.14.4 Authorize Printer Maintenance Record

This topic provides the systematic instructions to authorize Printer Maintenance record.

Authorize an unauthorized Printer Maintenance Record in the system for it to be processed as follows:

1. Start the **Printer Maintenance Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

    All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

    The **Printer Maintenance** screen is displayed.

5. 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.

1.14.5 Amend Printer Maintenance Record

This topic provides the systematic instructions to amend Printer Maintenance record.

Modify the details of an authorized record using the **Unlock** operation from the Action List. To make changes to a record after authorization:

1. Start the **Printer Maintenance Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for amendment.

    You can only amend authorized records.

3. Specify any or all of the details and click **Search** button.

    All records with the specified details are retrieved and displayed in the screen.

4. Double-click the record that you wish to amend.

    The **Printer Maintenance** screen is displayed.

5. Select **Unlock** operation from the Action List to amend the record.

6. Amend the necessary information and click **Save** to save the changes.

1.14.6 Authorize Amended Printer Maintenance Record

This topic provides the systematic instructions to authorize amended Printer Maintenance record.

Authorize an amended Printer Maintenance Record 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 process of subsequent authorization is the same as that for normal transactions.

1.15 Process Row Level Security Maintenance

This topic provides the systematic instructions to enable or disable Row Level Security (RLS) policy.

1. On **Home** screen, type **UTDRLSMT** in the text box, and click **Next**.

    The **Row Level Security Maintenance** screen is displayed.

    Figure 1-21   Row Level Security Maintenance

2. On **Row Level Security Maintenance** screen, click **New** to enter the details.

    For more information on fields, refer to the field description table.

    Table 1-19   Row Level Security Maintenance - Field Description

Field	Description
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**
Execute Query button	Click **Execute Query** to display the following details: • **Policy Name** • **Table Name** • **Policy Function**

Table 1-19   (Cont.) Row Level Security Maintenance - Field Description

Field	Description
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

Enable Auto Authorization

This topic explains why authorization is required and how to enable auto authorization and its features.

Normal Process of Authorization

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

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

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

Auto-authorization

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:

Table 2-1   Features and Auto-authorization Facility

Features	Auto-authorization Facility
Enable Auto-authorization Features for Business Users	The 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.

Table 2-1   (Cont.) Features and Auto-authorization Facility

Features	Auto-authorization Facility
Enable Auto-authorization Features for a User Group	The 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.
Enable Auto-authorization Features for Data Operations	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.

This topic contains the following sub-topics:

*   Using Auto-Authorization Feature
    This topic gives information on using Auto-Authorization Feature.

*   Process Auto Auth
    This topic provides the systematic instructions to map user groups to the tasks for which auto-authorization is applicable.

*   Enable or Disable Auto-authorization for a User Group
    This topic provides instructions to enable or disable Auto-authorization feature for a User Group.

*   Set up Auto Auth screen based on Fund and RPO code
    This topic gives instructions to set up Auto Auth screen based on Fund and RPO code.

*   Operations on Auto Authorization Records
    This topic provides the systematic instructions to perform the basic operations on the selected records.

2.1 Using Auto-Authorization Feature

This topic gives information on using Auto-Authorization Feature.

You must map the user groups to the menu items or the task for which auto-authorization is applicable to allow the auto-authorization feature for a user group and a certain set of menu items using the **Auto Auth** 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.

Table 2-2   Priority and Auto-Authorization

Priority	Auto-Authorization
First	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**.
Second	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.
Third	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.

2.2 Process Auto Auth

This topic provides the systematic instructions to map user groups to the tasks for which auto-authorization is applicable.

1. On **Home** screen, type **SMDAUTAU** in the text box, and click **Next**.

   The **Auto Auth** screen is displayed.

Figure 2-1   Auto Auth

2. On **Auto Auth** screen, click **New** to enter the details.

For more information on fields, refer to the field description table.

Table 2-3   Auto Auth - Field Description

Field	Description
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 displays 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	The section displays the following fields.
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.

2.3 Enable or Disable Auto-authorization for a User Group

This topic provides instructions to enable or disable Auto-authorization feature for a User Group.

1. Process the **Auto Auth** screen.

   The auto authorization features that have been enabled for the module and the group to which the logged in user belongs, are displayed.

2. Click **Modify** to amend the displayed list.

   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.

   The screen is displayed in Amend mode, where you can make your changes.

3. You can make changes to enable auto-authorization as follows:

   - Select **YES** in the **New** field for the task item to enable auto-authorization in the `New` mode for a task item.

   - Select **YES** in the **Modify** field for the task item to enable auto-authorization in the Amend mode for a task.

4. You can limit the volume of the transactions that can be auto-authorized for transaction data entry task items. To setup this limit:

   You can indicate a different limit for each role or Group ID, if necessary.

   a. Specify the highest volume of the transaction that can be auto-authorized, in the **Limit Amount** field.

   b. Indicate the currency in which the volume you have specified is reckoned, in the **Limit Currency** field.

5. You can also enable (or disable) the auto authorization feature for transactions in the **Additional Setup Details** section in the following circumstances:

   - **BackDated Transactions:** Select `BackDated Transaction` in the **Restricted Transaction** field to disable auto authorization of backdated transactions in the selected mode. Else, auto-authorization is enabled for backdated transactions in the selected mode.

   - **Load Overridden Transactions:** Transactions in respect of which applicable loads have been overridden. Select `Load Overridden Transaction` in the **Restricted Transaction** field to disable auto authorization of load override transactions in the selected mode. Else, auto-authorization is enabled for load overridden transactions in the selected mode.

   - **Third Party Payment Transactions:** Transactions for which third party payment has been specified. Select `Third Party Payment Transaction` in the **Restricted Transaction** field to disable auto authorization of third party payment transactions in the selected mode. Else, auto-authorization is enabled for third party payment transactions in the selected mode.

   - **Third Party Delivery Transactions:** Transactions for which third party delivery has been specified. Select `Third Party Delivery Transaction` in the **Restricted Transaction** field to disable auto authorization of third party delivery transactions in the selected mode. Else, auto-authorization is enabled for third party delivery transactions in the selected mode.

6. Click **Save** when you have finished making the auto-authorization specification for a user group 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.

7. Click **Save** to enable auto authorization for a user group other than the logged in user group in the **Auto Auth** screen.

   The system displays the message as `Do you want to cancel the operation?`.

8. Click **Ok** button.

   The auto authorization record of the logged in user group, which was on display, is closed, and the **Auto Auth** screen is opened in **New** mode.

9. Select the user group for which you want to enable or disable the auto authorization rights in the **Group ID** field.

10. Select the corresponding module in the **Module ID** field and click **Ok** button.

11. Subsequently, proceed to set up the auto authorization rights in the same manner for **New** mode as described above for the Amend mode.

2.4 Set up Auto Auth screen based on Fund and RPO code

This topic gives instructions to set up Auto Auth screen based on Fund and RPO code.

You can set up **Auto Auth** screen 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:

Table 2-4   Auto Auth set up table

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:

Table 2-5   Auto Auth set up table

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

2.5 Operations on Auto Authorization Records

This topic provides the systematic instructions to perform the basic operations on the selected records.

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

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

3. You can only make changes to any of the details through an amendment after authorization.

4. You can use the **Auto Auth** screen for the following operations on auto authorization setup:

   • Retrieval for viewing

   • Editing unauthorized setup

   • Deleting unauthorized setup

   • Authorizing setup

   • Amending authorized setup

5. Click the appropriate buttons in the **Auto Auth** screen to perform these operations.

3

External System Maintenance

This topic explains about the maintenance of an external system that will communicate with FCIS.

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 topic contains the following sub-topics:

- Process External System Details
  This topic provides the systematic instructions to maintain an external system that will communicate with **FCIS**.

- External System Summary
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- Process External System Functions Details
  This topic provides the systematic instructions to define access rights to an external system.

- External System Functions Summary
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- Process Message Media Detail
  This topic provides the systematic instructions to maintain message media.

- Message Media Summary
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- Process Media Control Systems Detail
  This topic provides the systematic instructions to maintain **Media Control Systems (MCS)**.

- Media Control Systems Summary
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- Process Amendment Details
  This topic provides the systematic instructions to maintain amendment details.

- **Amendment Maintenance Summary**
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- **Process Integration Parameter Maintenance**
  This topic provides the systematic instructions to maintain integration parameter.

- **Process Upload Source Maintenance**
  This topic provides the systematic instructions to maintain the details of the source from which data has to be uploaded.

- **Upload Source Summary**
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- **Process Source Preferences Maintenance**
  This topic provides the systematic instructions to set preferences for upload of data from an external source.

- **Source Preferences Summary**
  This topic provides the systematic instructions to perform the basic operations on the selected records.

- **Process Notification Enroute Maintenance**
  This topic provides the systematic instructions to set up notification queue at the module level.

- **Process Notifications Installed Maintenance**
  This topic provides the systematic instructions to maintain installed notifications.

3.1 Process External System Details

This topic provides the systematic instructions to maintain an external system that will communicate with **FCIS**.

1. On **Home** screen, type **UTDEXSYS** in the text box, and click **Next**.

   The **External System Details** screen is displayed.

   Figure 3-1   External System Details

2. On **External System Details** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 3-1   External System Details - Field Description

Field	Description
External System	The section displays the following fields.
External System	*Alphanumeric; 12 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	The section displays the following fields.
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	The section displays the following fields.
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	The section displays the following fields.
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**.

Table 3-1   (Cont.) External System Details - Field Description

Field	Description
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	The section displays the following fields.
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**.

3.2 External System Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve External System Details

1. On **Home** screen, type **UTSEXSYS** in the text box, and click **Next**.

    The **External System Summary** screen is displayed.

Figure 3-2   External System Summary

2. On **External System Summary** screen, specify any or all of the following details in the corresponding fields:

   - **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   - **Record Status**

   - **External System**

   - **Dead Letter Queue**

   - **Default Response Queue**

3. Click **Search** button to view the records.

   All the records with the specified details are retrieved and displayed in 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 **External System**
   > - Press F8

4. Perform **Edit**, **Delete**, **Amend**, **Authorize**, **Reverse**, and **Confirm** operations by selecting the desired operation from the Action list. You can also search a record by using a 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.

- • Edit External System Details
  This topic provides the systematic instructions to edit External System details.

- • View External System Details
  This topic provides the systematic instructions to view External System details.

- • Delete External System Details
  This topic provides the systematic instructions to delete External System details.

- • Authorize External System Details
  This topic provides the systematic instructions to authorize External System details.

3.2.1 Edit External System Details

This topic provides the systematic instructions to edit External System details.

Modify the details of External System that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **External System Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

   All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

   The **External System Details** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. Click **Save** to save your changes.

   The **External System Details** screen is closed and the changes made are reflected in the **External System Summary** screen.

3.2.2 View External System Details

This topic provides the systematic instructions to view External System details.

View a record that you have previously input by retrieving the same in the **External System Summary** screen. Perform this operation as follows:

1. Start the **External System Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **External System Details** screen is displayed.

3.2.3 Delete External System Details

This topic provides the systematic instructions to delete External System details.

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

1. Start the **External System Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **External System Details** screen is displayed.

5. 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.

3.2.4 Authorize External System Details

This topic provides the systematic instructions to authorize External System details.

Authorize an unauthorized External System Details in the system for it to be processed as follows:

1. Start the **External System Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **External System Details** screen is displayed.

5. 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.

3.3 Process External System Functions Details

This topic provides the systematic instructions to define access rights to an external system.

1. On **Home** screen, type **UTDEXFUN** in the text box, and click **Next**.

   The **External System Functions Details** screen is displayed.

   Figure 3-3   External System Functions Details

2. On **External System Functions Details** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

   Table 3-2   External System Functions Details - Field Description

Field	Description
External System	The section displays the following fields.
External System	*Alphanumeric; 12 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**.

3.4 External System Functions Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve External System Functions Details

1. On **Home** screen, type **UTSEXFUN** in the text box, and click **Next**.

   The **External System Functions Summary** screen is displayed.

Figure 3-4   External System Functions Summary

2. On **External System Functions Summary** screen, specify any or all of the following details in the corresponding fields:

   • **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   • **Record Status**

   • **External System**

   • **Function**

   • **Action**

3. Click **Search** button to view the records.

   All the records with the specified details are retrieved and displayed in the screen.

   • Edit External System Functions Details
     This topic provides the systematic instructions to edit External System Functions details.

   • View External System Functions Details
     This topic provides the systematic instructions to view External System Functions details..

   • Delete External System Functions Details
     This topic provides the systematic instructions to delete External System Functions details..

- Authorize External System Functions Details
  This topic provides the systematic instructions to authorize External System Functions details..

3.4.1 Edit External System Functions Details

This topic provides the systematic instructions to edit External System Functions details.

Modify the details of External System Functions that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **External System Functions Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

   All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

   The **External System Functions** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. Click **Save** to save your changes.

   The **External System Functions** screen is closed and the changes made are reflected in the **External System Functions Summary** screen.

3.4.2 View External System Functions Details

This topic provides the systematic instructions to view External System Functions details..

View a record that you have previously input by retrieving the same in the **External System Functions Summary** screen. Perform this operation as follows:

1. Start the **External System Functions Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **External System Functions** screen is displayed in View mode.

3.4.3 Delete External System Functions Details

This topic provides the systematic instructions to delete External System Functions details..

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

1. Start the **External System Functions Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **External System Functions** screen is displayed.

5. 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.

3.4.4 Authorize External System Functions Details

This topic provides the systematic instructions to authorize External System Functions details..

Authorize an unauthorized External System Functions Details in the system for it to be processed as follows:

1. Start the **External System Functions Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **External System Functions** screen is displayed.

5. 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.

3.5 Process Message Media Detail

This topic provides the systematic instructions to maintain 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 using this screen.

1. On **Home** screen, type **UTDMEDIA** in the text box, and click **Next**.

   The **Message Media Detail** screen is displayed.

   Figure 3-5   Message Media Detail

2. You can maintain the following in this screen:

   • 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.

3. On **Message Media Detail** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

   Table 3-3   Printer Maintenance - Field Description

Field	Description
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.

Table 3-3   (Cont.) Printer Maintenance - Field Description

Field	Description
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.

3.6 Message Media Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve Message Media Details

1. On **Home** screen, type **UTSMEDIA** in the text box, and click **Next**.

   The **Message Media Summary** screen is displayed.

Figure 3-6   Message Media Summary

2. On **Message Media Summary** screen, specify any or all of the following details in the corresponding fields:

   - **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   - **Record Status**

   - **Media Code**

   - **Description**

   - **Media Number**

3. Click **Search** button to view the records.

   All the records with the specified details are retrieved and displayed in 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 **Media Code/Number**
   >
   > - Press F8

- Edit Message Media Details
  This topic provides the systematic instructions to edit Message Media details.

- View Message Media Details
  This topic provides the systematic instructions to view Message Media details.

- Delete Message Media Details
  This topic provides the systematic instructions to delete Message Media details.

- Authorize Message Media Details
  This topic provides the systematic instructions to authorize Message Media details.

3.6.1 Edit Message Media Details

This topic provides the systematic instructions to edit Message Media details.

Modify the details of Message Media that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **Message Media Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

   All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

   The **Message Media Detail** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. Click **Save** to save your changes.

   The **Message Media Detail** screen is closed and the changes made are reflected in the **Message Media Summary** screen.

3.6.2 View Message Media Details

This topic provides the systematic instructions to view Message Media details.

View a record that you have previously input by retrieving the same in the **Message Media Summary** screen. Perform this operation as follows:

1. Start the **Message Media Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **Message Media Detail** screen is displayed in View mode.

3.6.3 Delete Message Media Details

This topic provides the systematic instructions to delete Message Media details.

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

1. Start the **Message Media Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **Message Media Detail** screen is displayed.

5. 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.

3.6.4 Authorize Message Media Details

This topic provides the systematic instructions to authorize Message Media details.

Authorize an unauthorized Message Media Details in the system for it to be processed as follows:

1. Start the **Message Media Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **Message Media Detail** screen is displayed.

5. 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.

3.7 Process Media Control Systems Detail

This topic provides the systematic instructions to maintain **Media Control Systems (MCS)**.

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.

1. On **Home** screen, type **UTDMCS** in the text box, and click **Next**.

   The **Media Control Systems Detail** screen is displayed.

Figure 3-7   Media Control Systems Detail

2. On **Media Control Systems Detail** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 3-4   Media Control Systems Detail - Field Description

Field	Description
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 Detail** 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.

Table 3-4   (Cont.) Media Control Systems Detail - Field Description

Field	Description

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** – 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.

Table 3-4   (Cont.) Media Control Systems Detail - Field Description

Field	Description
WebSphere Messaging	*Optional* Check this option to select WebSphere messaging.

3.8 Media Control Systems Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve Media Control Systems Details

1. On **Home** screen, type **UTSMCS** in the text box, and click **Next**.

   The **Media Control Systems Summary** screen is displayed.

Figure 3-8   Media Control Systems Summary

2. On **Media Control Systems Summary** screen, specify any or all of the following details in the corresponding fields:

   • **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   • **Record Status**

   • **Node**

   • **Media Control System**

   • **Media**

3. Click **Search** button to view the records.

   All the records with the specified details are retrieved and displayed in 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 Node/Media Control System/Media
>
> • Press F8

• Edit Media Control Systems Details
  This topic provides the systematic instructions to edit Media Control Systems details.

• View Media Control Systems Details
  This topic provides the systematic instructions to view Media Control Systems details.

• Delete Media Control Systems Details
  This topic provides the systematic instructions to delete Media Control Systems details.

• Authorize Media Control Systems Details
  This topic provides the systematic instructions to authorize Media Control Systems details.

3.8.1 Edit Media Control Systems Details

This topic provides the systematic instructions to edit Media Control Systems details.

Modify the details of Media Control Systems that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **Media Control Systems Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

   All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

   The **Media Control Systems Detail** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. Click **Save** to save your changes.

   The **Media Control Systems Detail** screen is closed and the changes made are reflected in the **Media Control Systems Summary** screen.

3.8.2 View Media Control Systems Details

This topic provides the systematic instructions to view Media Control Systems details.

View a record that you have previously input by retrieving the same in the **Media Control Systems Summary** screen. Perform this operation as follows:

1. Start the **Media Control Systems Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **Media Control Systems Detail** screen is displayed in View mode.

3.8.3 Delete Media Control Systems Details

This topic provides the systematic instructions to delete Media Control Systems details.

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

1. Start the **Media Control Systems Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **Media Control Systems Detail** screen is displayed.

5. 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.

3.8.4 Authorize Media Control Systems Details

This topic provides the systematic instructions to authorize Media Control Systems details.

Authorize an unauthorized Media Control Systems Details in the system for it to be processed as follows:

1. Start the **Media Control Systems Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **Media Control Systems Detail** screen is displayed.

5. 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.

3.9 Process Amendment Details

This topic provides the systematic instructions to maintain amendment details.

FCIS facilitates maintenance of nodes and fields which are amended through external system.

1. On **Home** screen, type **UTDAMDMT** in the text box, and click **Next**.

   The **Amendment Details** screen is displayed.

Figure 3-9   Amendment Details

2. On **Amendment Details** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 3-5   Amendment Details - Field Description

Field	Description
External System	*Alphanumeric; 12 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.

Table 3-5   (Cont.) Amendment Details - Field Description

Field	Description
Operation Code	*Alphanumeric; 50 Characters; Optional* Select the operation code from the adjoining option list.
Amend Nodes	The section displays the following fields.
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	The section displays the following 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.

3.10 Amendment Maintenance Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve Amendment Maintenance Details

1. On **Home** screen, type **UTSAMDMT** in the text box, and click **Next**.

   The **Amendment Maintenance Summary** screen is displayed.

Figure 3-10   Amendment Maintenance Summary

2. On **Amendment Maintenance Summary** screen, specify any or all of the following details in the corresponding fields:

   • **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   • **Record Status**

   • **External System**

   • **Operation**

3. Click **Search** button to view the records.

   All the records with the specified details are retrieved and displayed in 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 External System/Operation
   >
   > • Press F8

• [Edit Amendment Maintenance Details](#)
This topic provides the systematic instructions to edit Amendment Maintenance details.

• [View Amendment Maintenance Details](#)
This topic provides the systematic instructions to view Amendment Maintenance details.

• [Delete Amendment Maintenance Details](#)
This topic provides the systematic instructions to delete Amendment Maintenance details.

• [Authorize Amendment Maintenance Details](#)
This topic provides the systematic instructions to authorize Amendment Maintenance details.

3.10.1 Edit Amendment Maintenance Details

This topic provides the systematic instructions to edit Amendment Maintenance details.

Modify the details of Amendment Maintenance that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **Amendment Maintenance Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

   All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

   The **Amendment Details** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. Click **Save** to save your changes.

   The **Amendment Details** screen is closed and the changes made are reflected in the **Amendment Maintenance Summary** screen.

3.10.2 View Amendment Maintenance Details

This topic provides the systematic instructions to view Amendment Maintenance details.

View a record that you have previously input by retrieving the same in the **Amendment Maintenance Summary** screen. Perform this operation as follows:

1. Start the **Amendment Maintenance Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **Amendment Details** screen is displayed.

3.10.3 Delete Amendment Maintenance Details

This topic provides the systematic instructions to delete Amendment Maintenance details.

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

1. Start the **Amendment Maintenance Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **Amendment Details** screen is displayed.

5. 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.

3.10.4 Authorize Amendment Maintenance Details

This topic provides the systematic instructions to authorize Amendment Maintenance details.

Authorize an unauthorized Amendment Maintenance Details in the system for it to be processed as follows:

1. Start the **Amendment Maintenance Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **Amendment Details** screen is displayed.

5. 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.

3.11 Process Integration Parameter Maintenance

This topic provides the systematic instructions to maintain integration parameter.

1. On **Home** screen, type **IFDINPRM** in the text box, and click **Next**.

   The **Integration Parameter Maintenance** screen is displayed.

Figure 3-11   Integration Parameter Maintenance

2. On **Integration Parameter Maintenance** screen, click **New** to enter the details.

For more information on fields, refer to the field description table.

Table 3-6   Integration Parameter Maintenance Screen - Field Description

Field	Description
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.

Table 3-6   (Cont.) Integration Parameter Maintenance Screen - Field Description

Field	Description
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 Class name.
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.

ORACLE

Table 3-6   (Cont.) Integration Parameter Maintenance Screen - Field Description

Field	Description
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.

3.12 Process Upload Source Maintenance

This topic provides the systematic instructions to maintain the details of the source from which data has to be uploaded.

The **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 **FCIS** using the **Upload Source Maintenance** screen.

1. On **Home** screen, type **SMDSORCE** in the text box, and click **Next**.

   The **Upload Source Maintenance** screen is displayed.

Figure 3-12   Upload Source Maintenance

2. On **Upload Source Maintenance** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 3-7   Upload Source Maintenance - Field Description

Field	Description
Source Code	*Alphanumeric; 12 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.

Table 3-7 (Cont.) Upload Source Maintenance - Field Description

Field	Description
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.

3.13 Upload Source Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve Upload Source Record

1. On **Home** screen, type **SMSSORCE** in the text box, and click **Next**.

   The **Upload Source Summary** screen is displayed.

Figure 3-13 Upload Source Summary

2. On **Upload Source Summary** screen, specify any or all of the following details in the corresponding fields:

   • **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   • **Record Status**

- **Source Code**

- **Description**

3. Click **Search** button to view the records.

All the records with the specified details are retrieved and displayed in 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

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

- Edit Upload Source Record
  This topic provides the systematic instructions to edit Upload Source record.

- View Upload Source Record
  This topic provides the systematic instructions to view Upload Source record.

- Delete Upload Source Record
  This topic provides the systematic instructions to delete Upload Source record.

- Authorize Upload Source Record
  This topic provides the systematic instructions to authorize Upload Source record.

- Amend Upload Source Record
  This topic provides the systematic instructions to amend Upload Source record.

- Authorize Amended Upload Source Record
  This topic provides the systematic instructions to authorize amended Upload Source record.

3.13.1 Edit Upload Source Record

This topic provides the systematic instructions to edit Upload Source record.

Modify the details of Upload Source Record that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **Upload Source Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

   The **Upload Source Maintenance** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. 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.

3.13.2 View Upload Source Record

This topic provides the systematic instructions to view Upload Source record.

View a record that you have previously input by retrieving the same in the **Upload Source Summary** screen. Perform this operation as follows:

1. Start the **Upload Source Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **Upload Source Maintenance** screen is displayed.

3.13.3 Delete Upload Source Record

This topic provides the systematic instructions to delete Upload Source record.

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

1. Start the **Upload Source Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **Upload Source Maintenance** screen is displayed.

5. 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.

3.13.4 Authorize Upload Source Record

This topic provides the systematic instructions to authorize Upload Source record.

Authorize an unauthorized Upload Source Record in the system for it to be processed as follows:

1. Start the **Upload Source Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **Upload Source Maintenance** screen is displayed.

5. 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.

3.13.5 Amend Upload Source Record

This topic provides the systematic instructions to amend Upload Source record.

Modify the details of an authorized record using the **Unlock** operation from the Action List. To make changes to a record after authorization:

1. Start the **Upload Source Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for amendment.

   You can only amend authorized records.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details are retrieved and displayed in the screen.

4. Double-click the record that you wish to amend.

   The **Upload Source Maintenance** screen is displayed.

5. Select **Unlock** operation from the Action List to amend the record.

6. Amend the necessary information and click **Save** to save the changes.

3.13.6 Authorize Amended Upload Source Record

This topic provides the systematic instructions to authorize amended Upload Source record.

Authorize an amended Upload Source Record 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 process of subsequent authorization is the same as that for normal transactions.

3.14 Process Source Preferences Maintenance

This topic provides the systematic instructions to set preferences for upload of data from an external source.

1. On **Home** screen, type **SMDUPLDM** in the text box, and click **Next**.

   The **Source Preferences Maintenance** screen is displayed.

Figure 3-14   Source Preferences Maintenance

2. On **Source Preferences Maintenance** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 3-8   Source Preferences Maintenance - Field Description

Field	Description
Source Code	*Alphanumeric; 12 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 Investor Servicing**.
Module Code	*Alphanumeric; 2 Characters; Mandatory*
	You can choose to upload data from a source directly onto a module in **Oracle FLEXCUBE Investor Servicing**.
	Indicate the module into which you would like to upload data from a given source.
Error Handling	The section displays the following fields.
On Override	*Mandatory*
	Oracle FLEXCUBE Investor Servicing 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

Table 3-8   (Cont.) Source Preferences Maintenance - Field Description

Field	Description
Exception	*Mandatory* In case a serious error occurs during data upload, **Oracle FLEXCUBE Investor Servicing** 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	The section displays the following fields.
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 Investor Servicing**, 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.

• Function Id Preferences Button
  This topic explains the **Function Id Preferences** button in the **Source Preferences Maintenance** screen.

3.14.1 Function Id Preferences Button

This topic explains the **Function Id Preferences** button in the **Source Preferences Maintenance** screen.

1. On **Source Preferences Maintenance** screen, click **Function Id Preferences** button to enter the details.

   The **Function** screen is displayed.

Figure 3-15   Source Preferences Maintenance_Function ID Preferences Button

2. On **Function** screen, specify the fields.

For more information on fields, refer to the field description table.

Table 3-9   Function - Field Description

Field	Description
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.

Table 3-9   (Cont.) Function - Field Description

Field	Description
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 Deferred Processing	*Optional* Check this box to allow deferred processing.
Allow EOD With Deferred	*Optional* Check this box to allow EOD with deferred record.

3.15 Source Preferences Summary

This topic provides the systematic instructions to perform the basic operations on the selected records.

Retrieve Source Preferences Record

1. On **Home** screen, type **SMSUPLDM** in the text box, and click **Next**.

   The **Source Preferences Summary** screen is displayed.

Figure 3-16   Source Preferences Summary

2. On **Source Preferences Summary** screen, specify any or all of the following details in the corresponding fields:

   • **Authorization Status** - If you choose the status, then the records matching the specified status are retrieved. If you do not choose any option, then all the records are retrieved.

   • **Record Status**

   • **Source Code**

   • **Status**

   • **On Override**

- **Module Code**

- **Exception**

3. Click **Search** button to view the records.

All the records with the specified details are retrieved and displayed in 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

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

- Edit Source Preferences Record
  This topic provides the systematic instructions to edit Source Preferences record.

- View Source Preferences Record
  This topic provides the systematic instructions to view Source Preferences record.

- Delete Source Preferences Record
  This topic provides the systematic instructions to delete Source Preferences record.

- Authorize Source Preferences Record
  This topic provides the systematic instructions to authorize Source Preferences record.

- Amend Source Preferences Record
  This topic provides the systematic instructions to amend Source Preferences record.

- Authorize Amended Source Preferences Record
  This topic provides the systematic instructions to authorize amended Source Preferences record.

3.15.1 Edit Source Preferences Record

This topic provides the systematic instructions to edit Source Preferences record.

Modify the details of Source Preferences Record that you have already entered into the system, provided it has not subsequently authorized. Perform this operation as follows:

1. Start the **Source Preferences Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details in the corresponding fields to retrieve the record that is to be modified.

4. Click **Search** button.

All unauthorized records with the specified details are retrieved and displayed in the screen.

5. Double-click the record that you want to modify in the list of displayed records.

   The **Source Preferences Maintenance** screen is displayed.

6. Select **Unlock** operation from the Action list to modify the record. Modify the necessary information.

7. 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.

3.15.2 View Source Preferences Record

This topic provides the systematic instructions to view Source Preferences record.

View a record that you have previously input by retrieving the same in the **Source Preferences Summary** screen. Perform this operation as follows:

1. Start the **Source Preferences Summary** screen from the Browser.

2. 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.

3. Specify any or all of the details of the record in the corresponding fields on the screen.

4. Click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

5. Double-click the record that you want to view in the list of displayed records.

   The **Source Preferences Maintenance** screen is displayed.

3.15.3 Delete Source Preferences Record

This topic provides the systematic instructions to delete Source Preferences record.

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

1. Start the **Source Preferences Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for deletion.

3. Specify any or all of the details and click **Search** button.

   All records with the specified fields are retrieved and displayed in the screen.

4. Double-click the record that you want to delete in the list of displayed records.

   The **Source Preferences Maintenance** screen is displayed.

5. 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.

3.15.4 Authorize Source Preferences Record

This topic provides the systematic instructions to authorize Source Preferences record.

Authorize an unauthorized Source Preferences Record in the system for it to be processed as follows:

1. Start the **Source Preferences Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for authorization. Typically, choose the **Unauthorized** option.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details that are pending authorization are retrieved and displayed in the screen.

4. Double-click the record that you wish to authorize.

   The **Source Preferences Maintenance** screen is displayed.

5. 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.

3.15.5 Amend Source Preferences Record

This topic provides the systematic instructions to amend Source Preferences record.

Modify the details of an authorized record using the **Unlock** operation from the Action List. To make changes to a record after authorization:

1. Start the **Source Preferences Summary** screen from the Browser.

2. Select the status of the record that you want to retrieve for amendment.

   You can only amend authorized records.

3. Specify any or all of the details and click **Search** button.

   All records with the specified details are retrieved and displayed in the screen.

4. Double-click the record that you wish to amend.

   The **Source Preferences Maintenance** screen is displayed.

5. Select **Unlock** operation from the Action List to amend the record.

6. Amend the necessary information and click **Save** to save the changes.

3.15.6 Authorize Amended Source Preferences Record

This topic provides the systematic instructions to authorize amended Source Preferences record.

Authorize an amended Source Preferences Record 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 process of subsequent authorization is the same as that for normal transactions.

3.16 Process Notification Enroute Maintenance

This topic provides the systematic instructions to set up notification queue at the module level.

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.

1. On **Home** screen, type **UTDNTFEN** in the text box, and click **Next**.

   The **Notification Enroute Maintenance** screen is displayed.

Figure 3-17   Notification Enroute Maintenance

2. On **Notification Enroute Maintenance** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

Table 3-10   Notification Enroute Maintenance - Field Description

Field	Description
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.

Table 3-10   (Cont.) Notification Enroute Maintenance - Field Description

Field	Description
Destination Name	*Alphanumeric; 100 Characters; Mandatory* Specify the destination name.

3.17 Process Notifications Installed Maintenance

This topic provides the systematic instructions to maintain installed notifications.

1. On **Home** screen, type **UTDNTFIN** in the text box, and click **Next**.

   The **Notifications Installed Maintenance** screen is displayed.

   Figure 3-18   Notifications Installed Maintenance

2. On **Notifications Installed Maintenance** screen, click **New** to enter the details.

   For more information on fields, refer to the field description table.

   Table 3-11   Notifications Installed Maintenance - Field Description

Field	Description
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.

Table 3-11   (Cont.) Notifications Installed Maintenance - Field Description

Field	Description
Description	*Display* The system displays the description for the selected notification code.

4

Tanking of Maintenance Records

This topic explains about the 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 topic contains the following sub-topics:

- Enable Tanking of Maintenance Records
  This topic explains on tanking of maintenance records.

- Tanking New and Modified Maintenance Records
  This topic explains on tanking New and Modified maintenance records.

4.1 Enable Tanking of Maintenance Records

This topic explains on 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:

Table 4-1   Function ID and Description

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 Maintenance	Detail	Campaign Maintenance
UTDCONPF	Country Preference	Detail	Country Preference Maintenance Detail
UTDCURCT	Currency Cut-Off	Detail	Currency Cut-off Detail
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

Table 4-1   (Cont.) Function ID and Description

FUNCTION_ID	MAIN_MENU	SUB_MENU_1	DESCRIPTION
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
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

Table 4-1   (Cont.) Function ID and Description

FUNCTION_ID	MAIN_MENU	SUB_MENU_1	DESCRIPTION
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
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

4.2 Tanking New and Modified Maintenance Records

This topic explains on tanking New and Modified maintenance records.

This topic contains the following sub-topics:

Table 4-2   Tanking New and Modified Maintenance Records

Tanking New and Modified Maintenance Records	Description
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.
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.
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.
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.
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.
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.
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.
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.

Index