Core User Manual
Oracle Banking Digital Experience Cloud Service
Release 25.1.0.0.0

Part No. G27932 -01

April 2025

ORACLE

Core User Manual

April 2025

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax:+91 22 6718 3001

www.oracle.com/financialservices/

Copyright © 2006, 2025, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

1. Preface 1–11

1.1 Purpose 1–11

1.2 Audience 1–11

1.3 Documentation Accessibility 1–11

1.4 Diversity and Inclusion 1–11

1.5 Conventions 1–11

1.6 Screenshot Disclaimer 1–12

1.7 Acronyms and Abbreviations 1–12

2. Dashboard 2-1

2.1 System Administrative Transactions 2-4

2.2 Administrative Maker Transactions 2-18

2.3 Administrative Approver Transactions 2-22

3. User Management 3-25

3.1 User Management - Create 3-27

3.2 User Management - Search and View 3-38

3.3 User Management - Edit 3-50

4. Party Preferences 4-1

4.1 Party Preferences- Search 4-2

4.2 Party Preferences - Create 4-5

4.3 Party Preferences- View 4-18

4.4 Party Preferences - Edit 4-23

5. Merchant Management 5-1

5.1 Merchant Management – Search 5-2

5.2 Merchant Management – Funds Out 5-5

5.3 Merchant Management – Collect Funds 5-12

5.4 Merchant Management - Delete 5-24

6. Limits Definition 6-1

6.1 Limits Definition - View 6-2

6.2 Limits Definition - Create 6-5

6.3 Limits Definition - Delete Limit 6-10

7. Limit Package Management 7-1

7.1 Limit Package Management - View 7-2

7.2 Limit Package Management - Create 7-7
7.3 Limit Package Management - Edit 7-11
7.4 Limit Package Management - Clone 7-16
7.5 Limit Package Management - Delete 7-19

8. User Limits 8-1
8.1 User Limits - View 8-2
8.2 User Limits - Edit 8-8

9. Transaction Group Maintenance 9-1
9.1 Transaction Group Maintenance - View 9-2
9.2 Transaction Group Maintenance - Create 9-4
9.3 Transaction Group Maintenance - Edit 9-5
9.4 Transaction Group Maintenance - Delete 9-8

10. Party Account Access 10-1
10.1 Party Account Access - Mapping (Create) 10-2
10.2 Party Account Access- View 10-9
10.3 Party Account Access- Edit 10-12
10.4 Party Account Access- Delete 10-16

11. User Account Access 11-1
11.1 User Account Access – View 11-2
11.2 User Account Access – Edit 11-7
11.3 User Account Access – Create 11-14
11.4 User Account Access – Delete 11-23

12. Party Resource Access 12-26
12.1 Party Resource Access - Mapping (Create) 12-27
12.2 Party Resource Access- View 12-31
12.3 Party Resource Access - Edit 12-34
12.4 Party Resource Access - Delete 12-37

13. User Resource Access 13-1
13.1 User Resource Access - Mapping (Create) 13-2
13.2 User Resource Access- Search 13-9
13.3 User Resource Access - Edit 13-14
13.4 User Resource Access - Delete 13-17

14. Approvals 14-1
14.1 Workflow Management 14-1

14.2 Approval Rules 14-24

15. Group Corporate Onboarding 15-1

15.1 Group Corporate Onboarding – Search Corporate 15-2

15.2 Step 1: Group Corporate Profiling 15-10

15.3 Step 2: Party Account Access 15-35

15.4 Step 3: User Onboarding 15-55

15.5 Step 4: User Group Maintenance 15-84

15.6 Step 5: User Account Access 15-93

15.7 Step 6: Report Mapping 15-121

15.8 Step 7: Workflow Management 15-132

15.9 Step 8: Approval Rules 15-144

16. Party Migration 16-179

17. Origination Workflow Configuration 17-1

17.1 View Workflow for a Single Product Application 17-2

17.2 Single Product Application 17-5

17.3 Bundle Application 17-7

18. Product Maintenance 18-16

18.1 Product Maintenance - View 18-17

18.2 Product Maintenance - Edit 18-20

18.3 Product Maintenance - Create 18-23

19. Analytics Dashboard 19-27

20. Resource Bundle Maintenance 20-34

20.1 Resource Bundle Maintenance - Search & View 20-34

20.2 Resource Bundle Maintenance - Edit 20-36

21. Feedback 21-37

21.1 Feedback Template Maintenance 21-37

21.2 Feedback Analytics 21-54

22. SMS Banking 22-1

22.1 SMS Banking - Edit 22-3

22.2 Missed Call Banking - Search 22-5

22.3 Missed Call Banking - Edit 22-7

23. System Rules 23-1

24. Timer Maintenance 24-7

24.1 View Timer 24-7
24.2 Update Timer 24-9

25. First Time Login 25-13

26. Transaction Aspects 26-1
26.1 View Transaction Aspects 26-2
26.2 Update Transaction Aspects 26-3

27. ATM / Branch Maintenance 27-1
27.1 ATM/ Branch Maintenance - Search 27-2
27.2 ATM/ Branch Maintenance - Add 27-5
27.3 ATM/ Branch Maintenance - Edit 27-13
27.4 ATM/ Branch Maintenance - Delete 27-15

28. Product Mapping 28-1
28.1 Product Mapping - View 28-2
28.2 Product Mapping - Edit 28-5
28.3 Product Mapping - Create 28-7

29. User Profile Maintenance 29-1
29.1 User Profile - View 29-2
29.2 User Profile - Edit 29-3

30. Payee Restriction Setup 30-1
30.1 Payee Restriction Setup - View 30-2
30.2 Payee Restriction Setup - Edit 30-5
30.3 Payee Restriction Setup - Create 30-8

31. Forex Deal Maintenance 31-1
31.1 Add Currency Pairs 31-1
31.2 Update Forex Deal 31-3

32. Touch Point Maintenance 32-2
32.1 Touch Point Maintenance - View 32-3
32.2 Touch Point Maintenance - Edit 32-6
32.3 Touch Point Maintenance - Create 32-8

33. Touch Point Group Maintenance 33-1
33.1 Touch Point Group Maintenance - View 33-1
33.2 Touch Point Group Maintenance - Edit 33-4
33.3 Touch Point Group Maintenance - Create 33-6

34. Role Maintenance 34-1
34.1 Search & View Application Role 34-2
34.2 Edit Application Role 34-7
34.3 Delete Application Role 34-11
34.4 Create Application Role 34-12

35. Entitlements 35-1
35.1 Entitlements - View 35-1
35.2 Entitlements - Edit 35-3

36. User Segment Maintenance 36-1
36.1 User Segment Maintenance - Search 36-2
36.2 User Segment Maintenance - Edit 36-6
36.3 User Segment Maintenance - Create 36-9

37. Authentication 37-1
37.1 Authentication - View 37-2
37.2 Authentication - Edit 37-7
37.3 Authentication - Create 37-11

38. Security Questions Maintenance 38-1
38.1 View Security Questions 38-2
38.2 Security Questions Maintenance - Edit 38-3
38.3 Security Questions Maintenance - Create 38-4

39. Security Keys 39-1
39.1 Password Encryption and Decryption with Public and Private Key Pairs 39-1
39.2 API Key 39-1
39.3 JWT Encryption Key 39-2

40. User Group - Subject Mapping 40-1
40.1 User Group - Subject Mapping - Search 40-2
40.2 User Group - Subject Mapping - Create 40-4
40.3 User Group - Subject Mapping - Modify 40-7

41. Alert Templates 41-1
41.1 View Alert Template 41-2
41.2 Create Alert Template 41-6
41.3 Update Alert Template 41-8
41.4 Delete Alert Template 41-10

42. Mailers 42-1

42.1 Mailers - Search and View 42-2
42.2 Mailers - Create 42-6
42.3 Mailers - Edit 42-9
42.4 Mailers - Delete 42-12

43. Account Aggregation 43-1
43.1 External Bank Maintenance 43-2

44. Spend Category 44-1
44.1 Spend Category - Search 44-2
44.2 Spend Category - Create 44-4
44.3 Spend Category - Edit 44-6

45. Goal Category Maintenance 45-1
45.1 Goal Category - Search 45-2
45.2 Goal Category - Create 45-6
45.3 Goal Category - Edit 45-8

46. Experience Builder 46-1
46.1 Experience 46-2
46.2 Mapping 46-17

47. Dashboard Overview 47-1
47.1 Dashboard Overview– Summary 47-3
47.2 Dashboard Overview– View 47-4
47.3 Dashboard Overview – Create 47-7
47.4 Dashboard Overview – Design – Create Administrator Template 47-11
47.5 Dashboard Overview – Edit 47-15
47.6 Dashboard Overview – Clone 47-17
47.7 Dashboard Overview – Delete 47-19
47.8 Dashboard Mapping – Summary 47-20

48. Relationship Maintenance 48-1
48.1 Relationship Mapping 48-1
48.2 Relationship Matrix 48-6

49. Transaction Blackout 49-1
49.1 Transaction Blackout - Search 49-2
49.2 Transaction Blackout - Create 49-5
49.3 Transaction Blackout - Edit 49-8
49.4 Transaction Blackout - Delete 49-11

50. Working Window 50-1
50.1 Transaction Working Window - Search 50-2
50.2 Transaction Working Window - Create 50-7
50.3 Transaction Working Window - Edit 50-12
50.4 Transaction Working Window - Delete 50-16

51. Audit Log 51-1
51.1 Search Audit Details 51-1

52. File Upload 52-1
52.1 File Identifier Maintenance 52-1
52.2 User File Identifier Mapping 52-25

53. User Group Management 53-1
53.1 User Groups – Select User Type 53-2
53.2 User Groups – Admin User 53-3
53.3 User Groups - Retail & Business User 53-8

54. Print Password 54-1
54.1 Print Password - Search 54-2
54.2 Print Password - Print 54-5

55. User Alerts Subscription 55-1
55.1 User Alerts Subscription - Search 55-2
55.2 Subscribe/ Unsubscribe Alerts 55-5

56. Group Corporate Alerts Subscription 55-8
56.1 Group Corporate Alerts Subscription - Search 55-9
56.2 Subscribe/ Unsubscribe Alerts 55-12

57. Request Processing 57–1
57.1 Request Processing - Summary 57–2
57.2 Service Request Details (For Service Requests available out of the box) 57–5
57.3 Service Request Details (Requests created using Service Request-Form Builder) 57–8

58. Terms and Conditions Maintenance 58–1
58.1 Terms and Conditions - Search and View 58–1
58.2 Create Terms and Conditions 58–5
58.3 Edit Terms and Conditions 58–6
58.4 Copy Terms and Conditions 58–7
58.5 Delete Terms and Conditions 58–9

59. Reports 59–1

60. Report Generation 60–1
60.1 Adhoc Reports 60–2
60.2 Schedule Reports 60–3
60.3 API Consumption Report 60–10
60.4 EPI Payment Reconciliation Report 60–20
60.5 FATCA & CRS Declaration Report 60–26
60.6 File Identifier wise Party User Mapping Report 60–40
60.7 Party User wise File Identifiers Mapping Report 60–46
60.8 Party wise File Identifiers Mapping Report 60–52
60.9 Approval Rule Report 60–58
60.10 User Segment Summary Report 60–62
60.11 User Entitlement Report 60–69
60.12 User List Report 60–1

61. My Reports 61–5
61.1 My Reports - Adhoc 61–5
61.2 My Reports - Scheduled 61–7

62. User Report Mapping 62–1
62.1 User Report Mapping – Select User Type 62–1
62.2 User Report Mapping - Administrator User 62–1
62.3 User Report Mapping – Retail and Business User 62–11

63. User Helpdesk 63–1

64. Mailbox 64–1
64.1 Mails 64–2
64.2 Alerts 64–12
64.3 Notifications 64–14

65. Security Settings 65–1
65.1 Set Security Question 65–1

66. Profile 66–1

67. Session Summary 67–1

68. Manage DND Alerts 68–1

69. Session Timeout 69–3

70. ATM & Branch Locator 70–1

1. Preface

1.1 Purpose

Welcome to the User Guide for Oracle Banking Digital Experience. This guide explains the operations that the user will follow while using the application.

1.2 Audience

This manual is intended for Customers and Partners who setup and use Oracle Banking Digital Experience.

1.3 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.

1.4 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.

1.5 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.

1.6 Screenshot Disclaimer

The images of screens used in this user manual are for illustrative purpose only, to provide improved understanding of the functionality; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.

1.7 Acronyms and Abbreviations

The list of the acronyms and abbreviations that you are likely to find in the manual are as follows:

Abbreviation	Description
OBDX	Oracle Banking Digital Experience

2. Dashboard

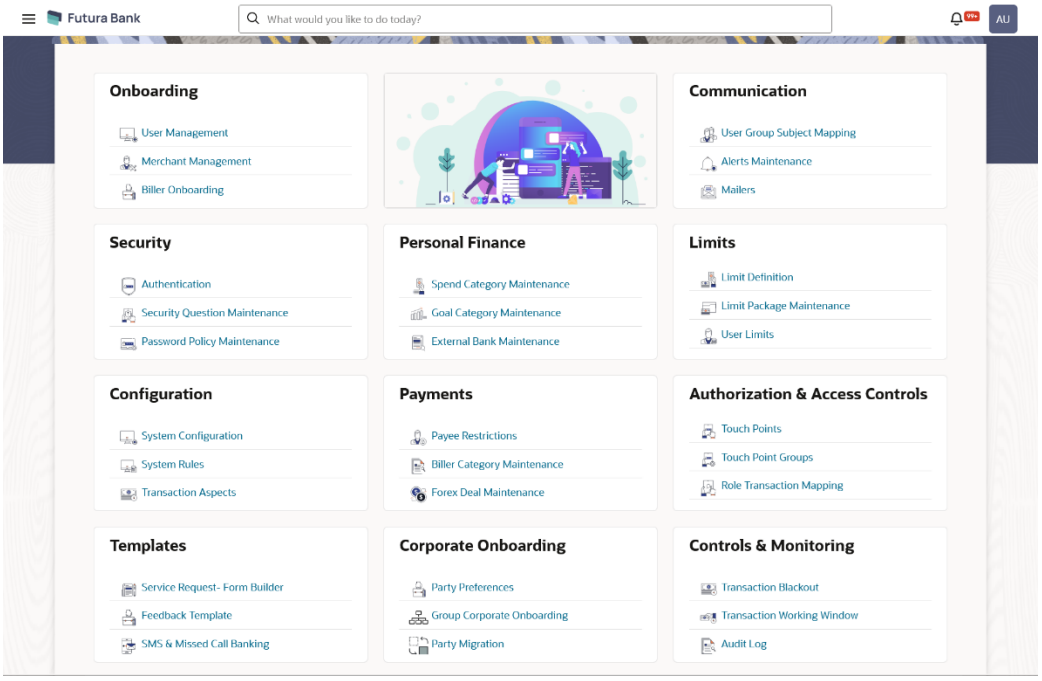
Dashboard allows an administrator user to access various administrative functions of the channel banking system. The role of the System/Bank administrator is to manage and administer day-to-day functions of a bank. Administrators can perform various tasks such as doing Day 1 maintenances, maintenances pertaining to retail / corporate banking, creation of roles, user creation, maintenance of party preferences etc.

Dashboards provides a quick view of the most relevant functions, to achieve a particular objective or complete a process. OBDX Administrator dashboard is mapped at various available levels like Party, Segment, User Type or User. This displays the end user's dashboard auto painted based on the roles assigned. The logged in-user can add or remove widgets while creating the dashboard. Each widget can be assigned a priority as per the requirement and the widgets to be displayed on the module dashboards will be based upon the assigned priority.

Note: All Administrative maintenances are supported only on 'Desktop' form factor and not supported on 'Mobile' and 'Tablet' .

The Administrator dashboard comprises of Quick Links, each of which when clicked launches into the respective item.

Dashboard



Dashboard Overview

Icons

Following icons are present on the System Administrator dashboard:

- : Clicking this icon takes you to the dashboard.
- : Click this icon and navigate to Mailbox or Alerts or Notifications screen.
- : Click this icon and enter the transaction name to search the transactions.
-

: Click this icon to view the user's profile and for logout option
- : Click the toggle menu to access the list of all the transactions.
- **Select Language**: Select your desired language from the drop-down list.
- **ATM & Branch Locator**: Click to view the address and location of the ATMs and the branches of the Bank.

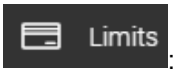
Toggle Menu Transactions

Following items are present on the Toggle Menu:

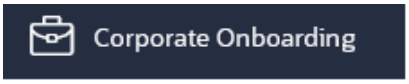
-

: Click this menu to access the configuration like System Rules, System Configuration, Transaction aspects etc.
-

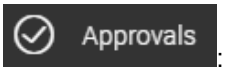
: Click this menu to setup access controls and authorization related transactions like maintain touch points, Application role creation and entitlement mapping etc.
-

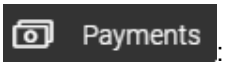
: Click this menu to access the security setup related transactions like setting up second factor authorization, password policy etc.
- 

: Click this menu to manage limits.
-

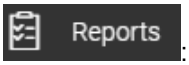
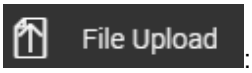
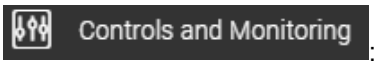
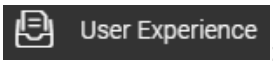
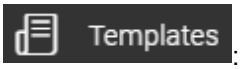
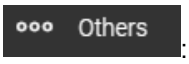
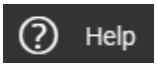
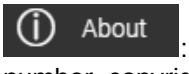
: Click this menu to onboard and manage, users, merchants
- 

: Click on this menu to onboard and manage Party and Group Corporates with Group corporate Profiling, Party Account Access ,User Management, User Group ,User Account Access, User Report Mapping, Approval Workflow & Rules
-

: Click this menu to set up account access rules for a corporate.
- 

: Click this menu to access and setup Approval workflow and rules for Corporate and Administrator users.
- 

: Click here to access maintenances with respect to payments.

- : Click this menu to plan finances and track expenditures. It consists of sub menu items like Spend Category Maintenance, Goal Category Maintenance and External Bank Maintenance.
-  : Click this menu to generate reports and view the generated reports.
-  : Click this menu to create a file identifier and map it to the user along with file upload and inquiry
- : Click this menu to access User Group Subject Mapping, Alert Maintenance and Mailers.
-  : Click this menu for controlling and monitoring the transactions like transaction blackout, working window and Audit log.
-  : Click this menu to manage and build your customize dashboards.
-  : Click this menu to manage service request form, feedback and SMS banking templates.
- : Click this menu to manage and limit the third party authorization access to an HTTP service.
-  : User Group Management, Print Password, User Alerts Subscription, Group Corporate Alerts Subscription, Request Processing and User Help Desk.
- : Click this menu to view the Mails, Alerts and Notifications.
- : Click this menu to view Pending for Approvals, My Initiated List, My Approved List
- : Click this menu to view the user's profile and login details like start date and time, end date and time, Channel and IP address of the last sessions of the logged in user.
- : Click to view the address and location of the ATMs and the branches of the Bank.
- : Click here to setup security questions and change password.
-  : Click this menu to launch the online help.
-  : Click this menu to view the information about the application like version number, copyright etc.

Note: The user will be shown the above options only if he has the access to the all the transactions falling under that group.

2.1 System Administrative Transactions

A System Administrator is responsible for setting up and maintaining the system. System Administrators are the members of the information technology department of the Bank who are mainly responsible for Bank's Day 1 maintenances or other day to day maintenances like Role Transaction Mapping, password policy maintenance and rules and roles maintenances etc.

Note: By default System Administrator role is given access to all the administrative functions. If the Bank wants to change the entitlements, the same can be done using Role Transaction Mapping function.

Following transactions are present on the System Administrator dashboard and in the menu:

- **On-boarding**

(a) User Management

User Management function enables the System Administrator to onboard and manage users along with their login credentials for channel banking access. This module facilitates channel banking access to the bank's internal users (administrators) and external users (customers).

User will get access to all the entities and clients mapped to it. Also the limit packages can get assigned once the user selects the accessible entities.

(b) Merchant Management

Merchant Management facilitates System Administrator to set up and maintain merchants using channel banking platform. This is to enable the customers to initiate merchant based payments using channel banking facility. This option allows the administrator to create / onboard new merchants, view existing merchants and modify their details, if required.

(c) Party Preferences (Through Toggle menu)

Party Preferences maintenance enables Bank administrator to define certain parameter values as per the corporate entities requirements. Following preferences can be set for a corporate party:

- Cumulative Daily/Monthly limits per transaction
- Transaction limits for users
- Approval flow – Parallel or Sequential or none
- To enable Channel access or not
- To enable Forex Deal creation or not
- To enable a Corporate Administrator or not.

(d) Group Corporate Onboarding

Group Corporate Onboarding maintenance enable the administrator to onboard the Group Corporate on OBDX in a single flow. Following steps can be followed during Group Corporate onboarding and send the same as a single approval:

- Group Corporate Profiling
- Party Account Access
- User Onboarding
- User Group
- User Account Access
- Report Mapping
- Workflow Management
- Approval Rules

Mapping of Parties belonging to different entities under a Group Corporate ID is allowed

- **Communications**

(a) User Group Subject Mapping

This maintenance facilitates mapping of subjects, to user groups in the bank, to streamline communication between the bank's users and its end customers.

Once User Groups are mapped to certain transactions or modules, users, in that group can reply to communication pertaining to the specific subject. The communication channel used is the bank's secure mailbox.

This option allows the System Administrator to search and view existing User Group – Subject mapping, modify the existing mapping and to create a new User Group – Subject mapping.

(b) Alert Maintenance

Alerts maintenance allows the System Administrator to define required parameters for each alert that is to be sent to the banks customers.

This option allows the System Administrator to search and view existing alerts, create a new alert and modify or delete an existing alert.

(c) Mailers

Mailers are information or a messages published by the Bank, to communicate about the Banks Products, services and other information to its users. A Bank may send mailers to announce a limited period promotional offer, launch of a product or service, etc.

The System Administrator creates Mailers which are sent to specific users, parties or user segments (all Retail / Corporate / Admin) users. Mailers can be customized to reach some or all users, to be sent now or on a specific date and time, in the future.

- **Configuration**

(a) System Configuration

Using this option System Administrator defines the basic components of this application which is necessary to run the application. The creating of system configuration is done at **'Day** 0' configuration.

(b) System Rules

System rules are defined to set different parameters for each enterprise role. The parameters that can be set for each enterprise role (Retail or Corporate Users) are Party Mapping, Limits Check, Party Preferences Check, Account Transaction Mapping, and Approvals Check, Group Corporate Check. If these parameters are enabled, application will check for a fulfillment of the maintenances, before final processing.

E.g. if **Approval check** flag is enabled for **'Corporate User'** type of enterprise role; then transactions initiated by corporate type of users will follow the approval maintenance for a party mapped to user and vice versa.

The flag **'Group Corporate'** is applicable only for **Corporate User'** type of enterprise role. This flag in System Rules screen defines the mode of corporate onboarding.

If **Group Corporate** flag is set **ON** then Bank administration will be able to onboard Group Corporate. The **Group Corporate** flag is enabled by default and always " When in the **Enterprise Role** field user type is selected as **Corporate User** then the **Group Corporate** flag will get displayed in non editable mode.

(c) Transactions Aspects

Using this option, System Administrator can define the aspects for a transaction. Depending on the aspects defined for a transaction through this maintenance, the transaction will be available/unavailable for selection in the respective maintenance screen.

User can view the aspects for a selected transaction and also edit the aspects i.e. enable/disable the aspects for the selected transaction.

(d) ATM/ Branch Maintenance

ATM Branch Locator feature available to the bank customers enables the users to locate the bank's ATMs/ branches available within a specific radius of his current location.

For the customers, to fetch the relevant information related to ATMs and Branches, system administrator maintains the data at their local databases. The basic details of ATMs and Branches are fetched from the core banking application, which is further enriched and stored in local database. This is a one-time activity at the time of implementation. Subsequently, as and when branches and ATMs are added, or any details regarding them updated, the administrator performs the necessary updates to the bank database.

Using this option, the System Administrator can search and view the ATM/ branch and its details (Fetched from Core Banking application) which include branch/ ATM id, branch name, address details, phone number, work timings and services offered by the bank. New ATM and branch details can also be manually added, viewed and edited.

The bank administrator can manually add new branch/ ATM details one by one, or add multiple branches / ATMs details simultaneously through file upload.

(e) Product Mapping

Product Mapping feature allows the System Administrator to map products with the channel. The business users will be able to access accounts related to the products mapped to the channel.

The System Administrator will be allowed to register the banks products to be made available to bank users for opening further accounts.

(f) User Profile Maintenance

This function enables the System/ Bank Administrator user to manage the user profile details that needs to be shown and needs to be made available for modification for Retail users. Details maintained on user profile includes date of birth, PAN card number, Aadhar number, passport number, national ID, driving license, communication address, email ID, and contact number, fax number, etc.

In a multi entity scenario, Administrator can do this setup for each entity by selecting the entity.

(g) First Time login

Using this option System administrator can configure the steps for banks business users to follow when the first-time login into the application. This step includes accepting Terms and Conditions, Setting up Security Questions, My profile, and limit information. The first-time login events are configurable at the Entity Level. Bank Admin would be able to define the mandatory and skippable steps for each entity. Post first-time login to the application, the system will check the configured steps for the logged-in entity and will be displayed to the user.

- **Security**

(a) Authentication

Passwords are the most common form of authentication used in the world today. But passwords are commonly forgotten and easily compromised. Two-factor authentication (2FA) adds an extra layer of security by requiring users to use two different authentication factors to verify user's identity.

The two step verification or Two Factor Authentication is an extra layer of security that is a subset of "multi factor authentication" that requires not only a password and username but also something that user has or something user knows or something they are e.g. tokens, OTP, biometrics etc. Using a Two Factor Authentication process can help to lower the number of cases of identity theft on the Internet, as well as phishing via email. For security reason authentication is used by user (Retail/ Corporate) while performing transactions through internet channel.

The two factor Authentication requires two different kinds of evidences before executing any transaction successfully. This option enables the system administrator to maintain authentication pattern for each transaction of a specific user segment.

The types of two factor authentication used in the application are as follows:

- Security Question
- Soft Token
- One Time Password (OTP)

(b) Security Question Maintenance

Application allows the System Administrator user to set up security questions, which will then be used as another layer of security (Over and above the Login credentials), before a user (Retail/ Corporate) can complete transactions through the internet channel.

Through the Manage Security Questions functionality, the administrator user can create and modify security questions that need to set and answered by user for completing any transaction. Administrator can add the security questions, if required.

(c) Password Policy Maintenance

Password policy maintenance enables System Administrator to define password parameters for users. Using this option System Administrator create, view and edit password policy for different user role/segments (Admin, Retail, and Corporate). Password policy maintenance contains following sections:

- **Password Validators:** This section contains the validations for a password. The validations include minimum and maximum length of the password, allowed characters in a password, repetitive and successive characters allowed, details to be excluded in the password like, date of birth, first and last name, user ID and party ID, and bank defined restricted passwords. User can also define number of successive incorrect attempts allowed, and number of previous password disallowed.
- **Password Expiry Parameters:** This section contains details about password expiry period, first password expiry period, and whether to force user to change password if there is a change in password policy (so that users can change their password as per the new password policy).

(d) Security Keys (Through Toggle menu)

Security key includes:

Password Encryption and Decryption with Public and Private Key Pairs:

Encryption and decryption allow communication between two parties to disguise information. The sender encrypts information before sending it and the receiver decrypts the information after receiving it. While in transit, the information is encrypted to ensure that it is protected from an intruder.

- Public and Private key pair helps to encrypt information that ensures sensitive data is protected during transmission. Whatever is encrypted with a Public Key can only be decrypted by its corresponding Private Key and vice versa.
- JWT Encryption Key: A JSON web token is a JSON object to represent a set of information. On sign in, user is authenticated and JWT token is generated. This JWT is subsequently passed to make API calls. To keep sensitive information hidden from the bearer (client) or third parties, JWT should be encrypted. A single key can be used to encrypt the data, if the JWT is encrypted with the key then the data can be decrypted using the same key.

- **Payments**

(a) Payee Restrictions

Payee Restriction Set up maintenance allows System Administrator to restrict the number of payees that a retail user can create for each payment network per day.

System Administrator can also restrict the total number of payees irrespective of payment network that the retail user can create per day.

This option allows the administrator to create payee restriction maintenance, View and Edit existing maintenance.

- **Personal Finance**

(a) Spend Category Maintenance

Using this option, the System Administrator can maintain the spend categories. Spend Category maintenance allows the administrator to create, modify or expire categories under which user can map expenses.

(b) Goal Category Maintenance

Goal Category maintenance allows the System Administrator to create, modify or expire goal categories. This maintenance is done only for Retail users and is not applicable to corporate.

The System Administrator created categories are linked with a product which will decide the other key parameters which will govern the Goal category. These parameters could be:

- Goal Amount Range (Minimum and Maximum Value)
- Interest Rate Offered
- Tenure Range (Minimum and Maximum)

The System Administrator can search and view goal categories, create a new goal category, and modify an existing goal category.

(c) **External Bank Maintenance**

The account aggregation feature empowers customers to view information of financial accounts that are external to OBDX, in addition to the customer's OBDX accounts. This feature also provides the customer with a consolidated view of accounts, net worth and recent transactions, across OBDX and external bank accounts.

To enable a retail user to access external bank accounts, and aggregate accounts with OBDX, the system administrator has to perform External Bank Maintenance

- **Authorization and Access Controls**

(a) Touch Points

Touch Points are different channels/ medium through which transactions or inquiries can be performed in OBDX. These can be created or modified under this section.

Touch Points in OBDX are of type 'Internal' and 'External'. Internal Touch Points are defined as part of Day 0 definition whereas External Touch Points are typically third party applications that can be defined by the System/ Bank Administrator as part of onboarding in OBDX

(b) Touch Points Groups

Touch Points are different channels e.g. Internet, Mobile, SMS, Third Party applications etc. through which the OBDX services can be accessed. This maintenance enables the System Administrator user to group two or multiple touch points together for the purpose of defining common limits for a transaction accessed from any touch point grouped together.

(c) Role Transaction Mapping

This function enables System Administrator to create Application Role and transaction mapping to application roles will be done for Touch Points. Administrator can create the application roles for the User Segments (Retail/ Corporate/ Administrator) and map the transactions to the application roles for internal as well as external touch points. The benefit of mapping the transactions on a touch point is that the Bank can control transaction access at each touch point.

(d) Entitlements

Entitlements are the transactions that the user can perform. Each Entitlement is linked to a single or group of resources.

Using this transaction user can view and edit the services and UI components linked to an entitlement for different actions i.e. Perform, Approve, and View.

(e) User Segment Maintenance

In order to offer appropriate product and services to the customers, banks can employ some method of segmentation. Banks can group customers into different segments based on different attributes of the customer; it could be demographic information, geographical information, behavioral information etc.

Banks can have different communication mailers, authentication mechanisms transaction limits and branding aspects based on customer segmentation.

User segment maintenance screen, allows the system administrator to create new segments and subsequently use these segments to define specific maintenances at user segment level. Limits can also be defined specific to a user segment. Within each user segment, limits package can be associated to different touch points.

- **Limits**

(a) Limit Definition

Limits are defined by the bank to set up amount and duration based restrictions on the transactions that can be carried out by the user.

As part of Limits Definition maintenance, the System Administrator can define:

- **Transaction Limits**: It is the initiation limit with minimum and maximum amount, defined typically for a user with role 'Maker'.
- **Cumulative Limits**: It is the collective transaction amount limit for all the transactions that can be performed during a day and maximum **number of transactions in a day.**
- **Cooling Period Limits:** It is the time set by the bank during which fund transfer is not allowed to a newly added payee.

This option allows the System Administrator to search and view limits, create limits and edit / delete existing limits.

(b) Limits Package Management

As part of the Limits Package definition, the created limits can be mapped to relevant transactions and/or roles.

The Limits Packages once created can be associated at User Level, Party Level and Role Level at an touch point level.

This option allows the System Administrator to search and view Limit Package, create a new Limit Package, and edit / delete existing Limit Package.

(c) Transaction Group Maintenance (Through Toggle menu)

Transaction group maintenance enables the System Administrator user to create and maintain group of transactions. Administrator can maintain a transaction group for the purpose of defining consolidated transaction limits. Once limits are assigned at transaction group, these limits acts as collective limit for selected transactions in a group.

(d) User Limits

This option allows the System Administrator to view the current available and utilized limits of specific retail user and also can modify (increase or decrease) the limits as per the requirement.

The user limits can be set for specific transaction level or at transaction group level or for a specific channel or for a group of channels.

The different types of limits are as follows:

- Daily Count- Permitted number of transactions in a day
- Daily Amount- Cumulative amount of transactions in a day
- Monthly Count- Permitted number of transactions in a month
- Monthly Amount- Permitted number of transactions in a month

- **Templates**

(a) Service Request Form Builder

Service Request Form Builder transaction allows the system administrator to define service requests by defining its attributes and by building the form (Request page that should be available to business user) which are then available for Retail users for creating a new Service Request.

(b) Feedback Template

Using this option, the System Administrator can maintain the feedback templates by defining the feedback question, selecting the rating scale, adding new questions along with new options, selecting the transactions for which feedback capture needs to be enabled.

The administrator can also decide whether an additional question is to be asked for a scale weight and select the applicable options for the question.

(c) SMS and Missed Call Banking

Using this option, the System Administrator can maintain the sms and missed call templates. The templates can be defined as:

- **SMS**: You can set the template / format of the message, which the account holder will be sending to the bank to receive the information in a specified format.
- **Missed Call**: You can set the template / format the account holder will receive, once he / she gives a miss call on the specified phone number.

(d) Experience Builder

Banks can have varied requirements with regards to the theme and for look and feel of the application.

Experience Builder is an administrative maintenance that allows the System Administrator to define the preferred theme for the application.

There is a list of categories on the left of the screen to choose from. System administrator can click and navigate the categories to upload their bank logo, select the preferred colours of the headers, back ground, Font, label, buttons etc. System administrator can also set the font style and font size.

(e) Dashboard Builder

Dashboard Builder is an administrative maintenance that allows the System Administrator to create and configure dashboard templates for Retail and Corporate users.

System Administrator can configure new dashboards by dragging and dropping the desired widget at desired location in template. And also can add and edit rows and columns while configuring new dashboard to add more widgets. Facility is also provided to search, view, edit and delete the configured dashboards.

These configured dashboards are responsive and can adapt to any type device that Bank wants to enable it to the customers' i.e. desktop, mobile and tablet. System allows the user to design new template and preview on different types of devices before enabling it.

The administrator can define multiple dashboards with the various attributes/ widgets. Further these templates can be mapped to the user segment, party or even to a specific user.

- **Controls & Monitoring**

(a) Transaction Blackout

The System Administrator can maintain a transaction blackout, for a period, when transaction/s are not accessible to users of the bank's retail and corporate or even to Bank administrators, for a preset time period.

The administrator may use the time, when a transaction is blacked-out, to do necessary maintenances.

Through this maintenance, the System Administrator can create a transaction blackout, User can search and view existing blackouts, and modify these if required. User can delete future dated blackouts.

(b) Transaction Working Window

A working window is maintained, by the System Administrator for each transaction for which a value date is applicable for processing. In order to enable such transactions on the channel, it is mandatory to define a working window for all the days of a week as Day 0 Maintenance. By performing this maintenance, the System Administrator defines the channel working window for each day of the week for a specific transaction.

Further, administrator can also define the processing pattern if the transaction is initiated by customers after the window is closed. Through this maintenance, the System Administrator can create a working window for a transaction, and also can create an exception to the normal window. User can search and view existing maintenances, and modify these if required.

(c) Audit Log

Audit log is set of records that provide information about operations performed in the application and details of the user who has performed it along with date and time when it was performed. The System Administrator can search and view the Audit Log.

(d) Feedback Analytics

Using this option, the System Administrator can analyze the feedback for different transactions. System Administrator can view top and bottom three transactions based on average customer review or he can search for individual transactions for a selected time period. Feedback Analytics gives the bank a quick analysis of the feedback information collected. The analytics covers information the average of feedback ratings transactions have got, trends in how the average ratings have changes, the top and bottom transactions in terms of ratings etc. The analytics helps banks in quickly identifying the pain points in customer journeys in the system points out the specific areas for improvement and action.
Using this option, the System Administrator can analyze the feedback given by users of the system.

(e) Relationship Mapping

Customer Relationship Maintenance enables the System Administrator to set up the transaction access logic for Bank's retail customers from Digital Banking Platform based on their account - mode of operation or relationship.

E.g. If a customer relationship (Mode of operation) is 'Either or Survivor', provide an access of all transactions whereas, if a customer relationship (Mode of operation) is 'Jointly', provide an access of all Inquiries and restrict all financial transactions from Digital Banking Platform. Such account and transaction access rules can be set up by the System Administrator using 'Relationship Maintenance Module'.

(f) Relationship Matrix

Relationship Matrix maintenance allows the System Administrator to define the transaction access based on the account relationships. Administrator can enable or disable each transaction for each relationship code. OBDX first checks if the transaction is enabled in a role attached to a user and then if it is enabled in relationship matrix. If both the conditions are satisfied, an access of a transaction and of an account is provided to the user.

Additional options accessible via Menu

- **Access Management**

Resource Access

(a) Party Resource Access

As part of Resource Access Management, administrator can define access on resources other than account like Remitter List from Virtual Account Management for a Corporate Party.

(b) User Resource Access

As part of Resource Access Management, administrator can define access on resources other than account like Remitter List from Virtual Account Management for a specific corporate user.

Approvals

(a) Workflow Management

Approval workflows are created to support requirements where multiple levels of approval are required in a specific sequence for a transaction/maintenance. Each workflow can be configured to have up to 5 levels of approval with a specific user or a user group configured at each level.

System Administrator can search and view approval workflows maintained and create new workflows. As a part of creating workflows, user can add various levels of approvals and map users or user groups to each level. User can also modify workflows maintained.

(b) Rules Management

The Administrator, can set up rules for approvals. Applying a rule makes the requirement for an approval more customized. For instance, through this screen, the bank administrator can create a rule, so that all administrator maintenances initiated by a certain user-group, always require approval.

- **Reports**

(a) Report Generation

Using this option, the System Administrator, can generate various adhoc reports. Application provides an option to generate reports using Oracle Analytics Publisher and / or by using an internal application.

(b) My Reports

On accessing 'My Reports' menu, the System Administrator, can view the last 10 reports generated with the respective report status. He can choose to search a specific report using the search criteria or can opt to view/ download detailed report.

(c) User Report Mapping

The user report mapping maintenance allows the Bank Administrators to map the report or set of reports to a specific corporate user. The corporate users can generate and view the reports which they have an access to.

Bank administrator searches a corporate user based on the party id and view the reports mapped to him, he can also un-map the reports from specific corporate user so that access of the specific report/ s can be removed to that corporate user.

The System Administrator can also map the accounts of primary and linked parties for which the reports can be generated by a corporate user, so that corporate user can generate the report only for the accounts mapped to him.

- **File Upload**

(a) File Identifier Maintenance

System Administrator, can create file identifiers (FI) for a corporate entity. A File Identifier is always mapped to a specific single file template. It permits configuration of corporate preferences like approval type (file level/ record level) for a particular type of file. This is a pre-requisite for the File Uploads functionality, for a corporate.

(b) User File Identifier Mapping

Through this option Administrator, can map a file identifier to a user to grant access rights to the user, for this specific file type. This maintenance enables a user to upload a specific file, approve the uploaded file and view its status. System administrator can map / un-map file identifiers to a User. Further, user can enable or disable the sensitive data check. This is a pre-requisite maintenance, for the File Uploads functionality, for a corporate.

(c) File Upload

This option allows the System administrator user to upload the files containing EBPP Billers. Billers uploaded will be available for retail users to register and make online bill payment & pre-paid recharge transactions.

(d) Uploaded File Inquiry

Through this option the user can view the Billers file uploaded and their status.

- The search can be filtered on various parameters like status and file reference ID.
- The user can track the status of the file and if there is an error in the file, he / she can download the error file to arrive at the exact reason for error.
- For files in the 'Processed' status, the user can download Response file, to vet status of processing (in the host) for each record, of the file.
- The user can track file history and also check Individual record details.

- **OAuth**

(a) Identity Domain Maintenance

The Identity Domain corresponds to the notion of a tenant and each identity domain corresponds to an identity store. All artifacts such as resource server and client needs to be created under an identity domain.

As part of the Identity Domain definition, Identity store as well as token settings can be defined.

Currently only 'Embedded LDAP' i.e. DB Authenticator as Identity Store is supported.

(b) Resource Server Maintenance

The resource server is the server that contains the user's information that is being accessed by the third party application and handles authenticated requests after the application has obtained an access token.

Resource Server is always associated to one Identity Domain. Through this maintenance, the administrator can define scopes for the resource server. Scopes are transactions or inquiries that are provided to the client so that the TPP/client can transact or inquire on behalf of the customer with an access token provided the customer has provided consent to the TPP.

(c) Client Maintenance

Clients are Third Party Provides (TPPs) that can access information from the resource server on behalf of the user provided the user has provided consent to the TPPs. As part of this definition, the administrator can define client details i.e. client ID, client name, scopes, redirect URLs etc.

- **Others**

(a) User Group Management

The System Administrator, can create administrator user groups with two or more users. User can search and views already maintained groups, and also modify these. The maintained administrator user groups are used for further maintenances like – User Group Subject Mapping or while creating approval rules.

(b) Print Password

When a new user opens an account in the bank and registers for internet banking, the bank sends the printed password along with some other documents like Welcome letter, Terms & Conditions document and applicable promotional offers to the registered user via courier or post. This screen allows the Bank Administrator to print the password along with these documents for new users as well as for existing users who have requested for reset password.

(c) User Alerts Subscription

The System Administrator, can subscribe users to mandatory alerts, through this option. In addition, Retail and Corporate users of the bank, can subscribe to alerts, and choose whether they want alerts delivered through Email, SMS or in their secured mailbox. The bank administrator processes the subscription request, received from customers. (For non-mandatory alerts).

(d) Request Processing

Service requests allows the System Administrator to search and view all the service requests that have been initiated by the Bank customers and are available with various statuses like Open, Completed and Rejected. Bank Administrator can search the service requests with specific search criteria and can update the status of open service requests.

(e) User Help Desk

This option enables the Administrator to create business user's session and perform the transaction requested by business user if he has forgotten his internet banking password or is unable to perform a transaction using his internet banking.

To authenticate the user, system will send an OTP to the customer and the same OTP needs to be communicated to the administrator user so that he can enter it on the screen to create user’s session.

(f) Message Maintenance

Using this option, System Administrator can inquire the existing Error Messages defined in the system for an OBDX error code. It also allows you to modify the text defined for a message code for a particular Language.

(g) Group Corporate Alert Subscription

Using this option the System/Bank Administrator can subscribe alerts at the Group Corporate level for selected events. The Bank Administrator subscribes the Corporate Party associated with Group Corporate to alerts, delivered through Email, SMS, through push notification or in their on-screen mailbox. This functionality is applicable for non-mandatory alerts.

- **Notifications**

The notification section allows the System Administrator user to view last 'N' number of notifications sent by the bank. Click **View All** to view all the notifications sent by the bank.

Note:
1) If the setup requires an approval workflow, it will be initiated. Once approved by the required number of approvers, the maintenance will be effective.

2) If the setup does not require an approval workflow or is self / auto approved, the maintenance will come into effect on confirmation.

2.2 Administrative Maker Transactions

Following transactions are available for the System Administrator in the dashboard and in the menu:

Bank Administrator Maker's role involves the maintenances which are mainly required for day to day business in banks. Maintenances like onboarding the users on Digital Platform and providing them the account and transactions access, etc.

Note: Transactions appearing in toggle menu for Bank Administrator – Maker is same as 'System Administrator' transactions depending upon the access provided to the associated role in Role Transaction Mapping maintenance.

On-boarding

(a) User Management

Bank Administrator can search and view users, create users and modify users. User can reset passwords of the users. Bank Administrator can also change the user status (lock/unlock) and grant/deny the channel access to a user, through this option.

(b) Party Preferences

Party Preferences maintenance enables Bank administrator to define certain parameter values as per the corporate entities requirements. Following preferences can be set for a corporate party:

- Cumulative Daily/Monthly limits per transaction
- Transaction limits for users
- Approval flow – Parallel or Sequential or none
- To enable Channel access or not
- To enable Forex Deal creation or not
- To enable a Corporate Administrator or not.
- Group Corporate Mapping.

(c) Group Corporate Onboarding

Group Corporate Onboarding maintenance enable the administrator to onboard the Group Corporate on OBDX in a single flow. Following steps can be followed during Group Corporate onboarding and send the same as a single approval:

- Group Corporate Profiling
- Party Account Access
- User Onboarding
- User Groups
- User Account Access
- Report Mapping
- Workflow Management
- Approval Rules

Mapping of Parties belonging to different entities under a Group Corporate ID is allowed

Approvals

(a) Workflow Management

Approval workflows are created to support requirements where multiple levels of approval are required in a specific sequence for a transaction/maintenance. Each workflow can be configured to have up to 5 levels of approval with a specific user or a user group configured at each level.

Bank Administrator Maker can search and view approval workflows maintained and create new workflows. As a part of creating workflows, user can add various levels of approvals and map users or user groups to each level. User can also modify workflows maintained.

(b) Rules Management

The Bank administrator – Maker, can set up rules, for approvals. Applying a rule makes the requirement for an approval more customized. For instance, through this screen, the bank administrator can create a rule, so that all administrator maintenances initiated by a certain user-group, always require approval.

Resource Access

(a) Party Resource Access

As part of Resource Access Management, administrator can define access on resources other than account like Remitter List from Virtual Account Management for a Corporate Party.

(b) User Resource Access

As part of Resource Access Management, administrator can define access on resources other than account like Remitter List from Virtual Account Management for a specific corporate user.

File Upload

(a) File Identifier Maintenance

Bank administrator – Maker, can create file identifiers (FI) for a corporate entity. A File Identifier is always mapped to a specific single file template. It permits configuration of corporate preferences like approval type (file level/ record level) for a particular type of file. This is a pre-requisite for the File Uploads functionality, for a corporate.

(b) User File Identifier Mapping

Through this option Bank Administrator – Maker, can map a file identifier to a user to grant access rights to the user, for this specific file type. This maintenance enables a user to upload a specific file, approve the uploaded file and view its status. Bank administrator maker can map / un-map file identifiers to a User. Further, user can enable or disable the sensitive data check. This is a pre-requisite maintenance, for the File Uploads functionality, for a corporate.

Origination Administrator

Others

(a) Request Processing

Service requests allows the Bank Administrator- maker to search and view all the service requests that have been initiated by the Bank customers and are available with various statuses like Open, Completed and Rejected. Bank Administrator can search the service requests with specific search criteria and can update the status of open service requests.

(b) Feedback

Using this option, the Administrator can maintain the feedback templates by defining the feedback question, selecting the rating scale, adding new questions along with new options, selecting the transactions for which feedback capture needs to be enabled.

The administrator can also decide whether an additional question is to be asked for a scale weight and select the applicable options for the question.

(c) User Help Desk

This option enables the Administrator to create business user's session and perform the transaction requested by business user if he has forgotten his internet banking password or is unable to perform a transaction using his internet banking.

To authenticate the user, system will send an OTP to the customer and the same OTP needs to be communicated to the administrator user so that he can enter it on the screen to create user’s session.

Note:

- If the setup requires an approval workflow, it will be initiated. Once approved by the required number of approvers, the maintenance will be effective.

- If the setup does not require an approval workflow or is self / auto approved, the maintenance will come into effect on saving and confirming.

1. Click **Back** to navigate to the **Dashboard**.

2.3 Administrative Approver Transactions

Bank administrator users can approve the transactions initiated by Bank administrator in maker role. Approver has the responsibility to ensure correctness of the maintenances as per the bank and corporate mandate, to ensure speedy and accurate processing.

Note: Toggle menu transactions of Bank Administrator – Approver is same as 'System Administrator' transactions depending on the access as provided to the user.

Transactions:

- Pending for Approval
- My Initiated List
- My Approved List

1) **Pending for Approval**

This section displays the details of transactions that are initiated by the maker and are pending for approval. User can click on transactions to view the details of transactions that are pending for approval.

The transactions pending approval within a period can be searched by providing a date range. Click on date picker icon to search the transactions based on Date range.

2) **My Initiated List**

Displays the list of all the administrative transactions initiated by the Administrator.

Date Picker: Click this icon to search the transactions that are performed on a particular date. A date range (**From Date** and **To Date)** can be provided to search the transaction.

3) **My Approved List**

This section displays the details of transactions that are approved by the approver user. Click on the transactions already approved to view the details with respective statuses and details.

The transactions that are approved within a period can be searched by providing a date range. Click on date picker icon to search the transactions based on Date range.

Date Picker:Click this icon to search the transactions that are approved on a particular date. A date range (**From Date** and **To Date)** can be provided to search the transaction.

Dashboard Overview

Pending for Approvals

The Bank Administrator – Approver, can view the items pending for his approval. For ease of use, he can expand this page.

Onboarding

(a) User Management

The Bank Administrator can search and view users, create users and modify users. User can reset passwords of the users. Also user can lock / unlock a user, through this option.

(b) Party Preferences

Party Preferences maintenance enables Bank Administrator to define certain parameter values as per the corporate entities requirements. Following preferences can be set for a corporate party:

- Cumulative Daily/Monthly limits per transaction
- Transaction limits for users
- Approval flow – Parallel or Sequential or none
- To enable Channel access or not
- To enable Forex deal or not
- To enable a Corporate Administrator or not.
- Group Corporate Mapping

(c) Group Corporate Onboarding

Group Corporate Onboarding maintenance enable the administrator to onboard the Group Corporate on OBDX in a single flow. Following steps can be followed during Group Corporate onboarding and send the same as a single approval:

- Group Corporate Profiling
- Party Account Access
- User Onboarding
- User Groups
- User Account Access
- Report Mapping
- Workflow Management
- Approval Rules

Approvals

(a) Workflow Management

Approval workflows are created to support requirements where multiple levels of approval are required in a specific sequence for a transaction/maintenance. Each workflow can be configured to have up to 5 levels of approval with a specific user or a user group configured at each level.

Bank Administrator Approver can search and view approval workflows maintained and create new workflows. As a part of creating workflows, user can add various levels of approvals and map users or user groups to each level. User can also modify workflows maintained.

(b) Rules Management

The Bank administrator – Approver, can set up rules, for approvals. Applying a rule makes the requirement for an approval more customized. For instance, through this screen, the Bank Administrator can create a rule, so that all administrator maintenances initiated by a certain user-group, always require approval.

Resource Access

(a) **Party Resource Access**

As part of Resource Access Management, administrator can define access on resources other than account like Remitter List from Virtual Account Management for a Corporate Party.

(b) User Resource Access

As part of Resource Access Management, administrator can define access on resources other than account like Remitter List from Virtual Account Management for a specific corporate user.

File Upload

(a) **File Identifier Maintenance**

Bank administrator – Approver, can create file identifiers (FI) for a corporate entity. A File Identifier is always mapped to a specific single file template. It permits configuration of corporate preferences like approval type (file level/ record level) for a particular type of file. This is a pre-requisite for the File Uploads functionality, for a corporate.

(b) User File Identifier Mapping

Through this option bank administrator – Approver, can map a file identifier to a user to grant access rights to the user, for this specific file type. This maintenance enables a user to upload a specific file, approve the uploaded file and view its status. Bank administrator Approver can map / un-map file identifiers to a User. Further, user can enable or disable the sensitive data check. This is a pre-requisite maintenance, for the File Uploads functionality, for a corporate.

Others

(a) Request Processing

Service requests allows the bank administrator- approver to search and view all the service requests that have been initiated by the maker and are pending for approvals. This option also allows him to approve or reject the service requests.

(b) Feedback

Using this option, the Administrator can maintain the feedback templates by defining the feedback question, selecting the rating scale, adding new questions along with new options, selecting the transactions for which feedback capture needs to be enabled.

The administrator can also decide whether an additional question is to be asked for a scale weight and select the applicable options for the question.

(c) User Help Desk

This option enables the Administrator to create business user's session and perform the transaction requested by business user on his behalf in case, he has forgotten his internet banking password or is unable to perform a transaction using his internet banking.

To authenticate the user, system will send an OTP to the customer and the same OTP needs to be communicated to the administrator user so that he can enter it on the screen to create user’s session.

3. User Management

User Management function enables System/ Bank Administrator to onboard and manage users and their login credentials for channel banking access. This module facilitates channel banking access to the bank's internal users (administrators) and external users (customers).

This function also lets the System/Bank Administrator to define the various touch points from which the user can access the channel banking and limit package applicable for the same.

Separate limits will be applicable for the transaction done by each Retail & Business party. For business party transactions, limit package maintained at the party level (as a part of party preference) will be considered and will be utilized. For retail party transactions, the limit package maintained at the user level will be considered and will be utilized.

Users can also be mapped to a User Segment, so that the attributes applicable at the segment level should get applied to the user. Currently user segments are only applicable for Retail users. Using this maintenance OBDX Bank administrator can onboard a user having Retail (Individual) and Business relationships with the bank to enable their digital banking accesses.

Note:
• User is created first in IDCS and then onboard in OBDX.
• One user can be assigned multiple business parties and a single retail party. Users will be able to log in with single user credentials to access the information of the user's business and personal accounts with the bank. Users will be provided with an option to switch between the parties to view the required information. No consolidated details across parties will be shown to the user.

The user details also shows the list all the user groups associated with a particular user. In order to remove a particular user from a user group, the administrator must manually go to the particular user group screen and remove the user.

In a multi entity scenario, this function enables system/ bank administrator to provide access to multiple entities to users.

Note :
• If Group Corporate Flag is set as "ON" in system rules, then the corporate user onboarding will not be allowed using this menu option. The Corporate User will be onboarded using Group Corporate onboarding only.
• Admin will be able to view the corporate user details and he can also change the corporate user status or the channel access permission for a user using this screen.
• If Group Corporate Flag is set as "OFF" in system rules, then the corporate user onboarding will be allowed using below mentioned steps.

Internal Users

- System Administrator
- Bank Administrator

External Users

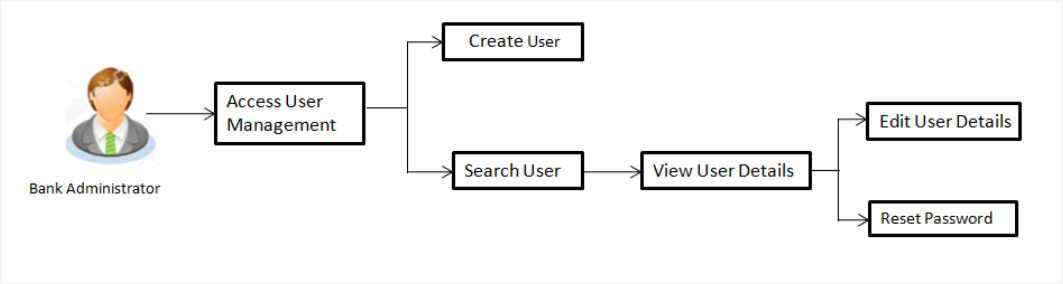
- Retail and Business User
- Corporate User

- Non Customer- Corporate users
- Corporate Administrator

Pre-Requisites

- User Segment and Application roles are maintained
- Transactions are associated with each Application role
- Transaction (User Management) access is provided to System/Bank Administrator.
- Approval rule set up for Bank administrator to perform the actions.
- Party Preference is maintained for corporate user

Workflow



Features Supported In Application

The User Management module allows the system/bank administrator to

- Create User
- View User
- Edit User
- Reset Password

How to reach here:

System/ Bank Administrator Dashboard > Onboarding > User Management
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Onboarding > User Management

---

Note: Non Customer Corporate users (for which the linked party id is not maintained in UBS or in Core banking system), can also be on boarded on OBDX. For such cases i.e. for non customer corporate users (counterparties on boarded by Corporates) the system will look for the party ID in OBSCF/OBCMS.

3.1 User Management - Create

System/Bank Administrator logs into the system and navigates to the User Management screen. This function allows the administrator to create internal and external users.

Administrators will be allowed to map one retail and multiple business parties within each entity. These parties will be considered at par with each other. While mapping a party, the Party Type also needs to be specified as Individual (Retail) or Business. If any of the party types is selected as 'Individual' then the user's personal and contact information will be fetched from the respective host system as read-only. If all the selected party (es) are of 'Business' type, then the administrator will be expected to fill the user's profile details manually.

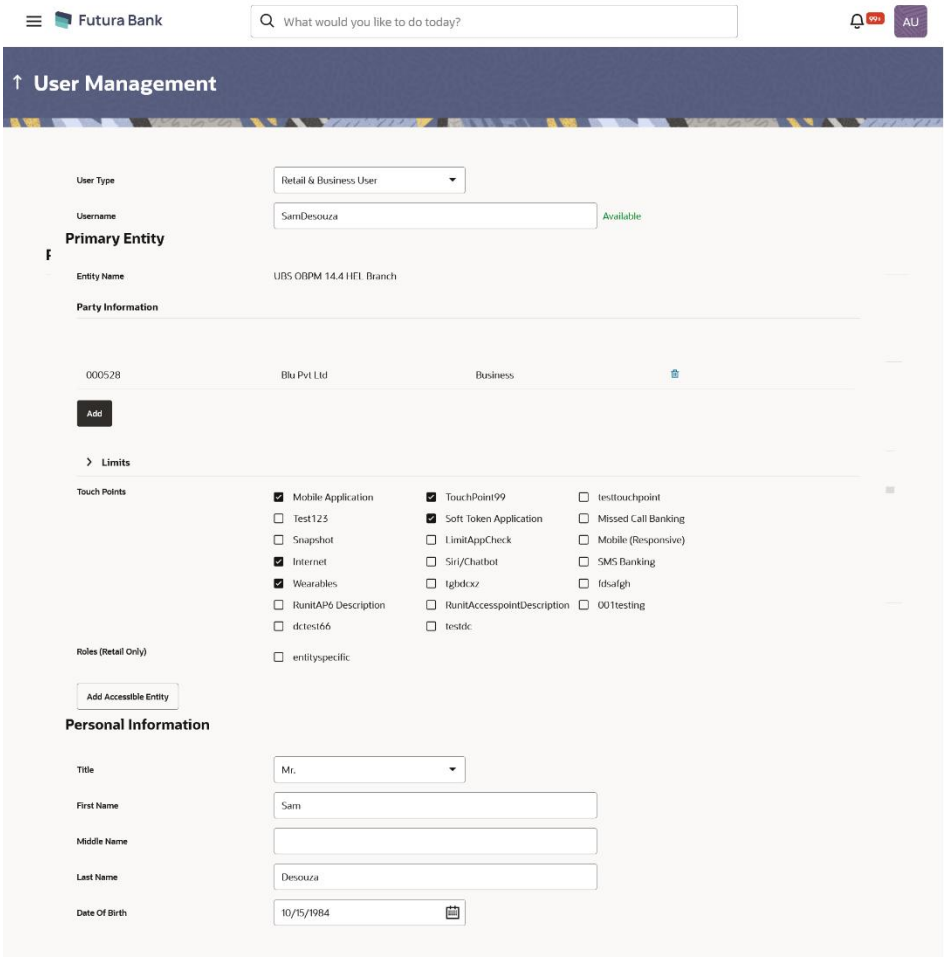
Segment and roles mapped at the user level will be applicable only to the user's retail profile. The segment will not be applicable for a business profile, and the roles mapped at the party preference level will be applicable for business parties.

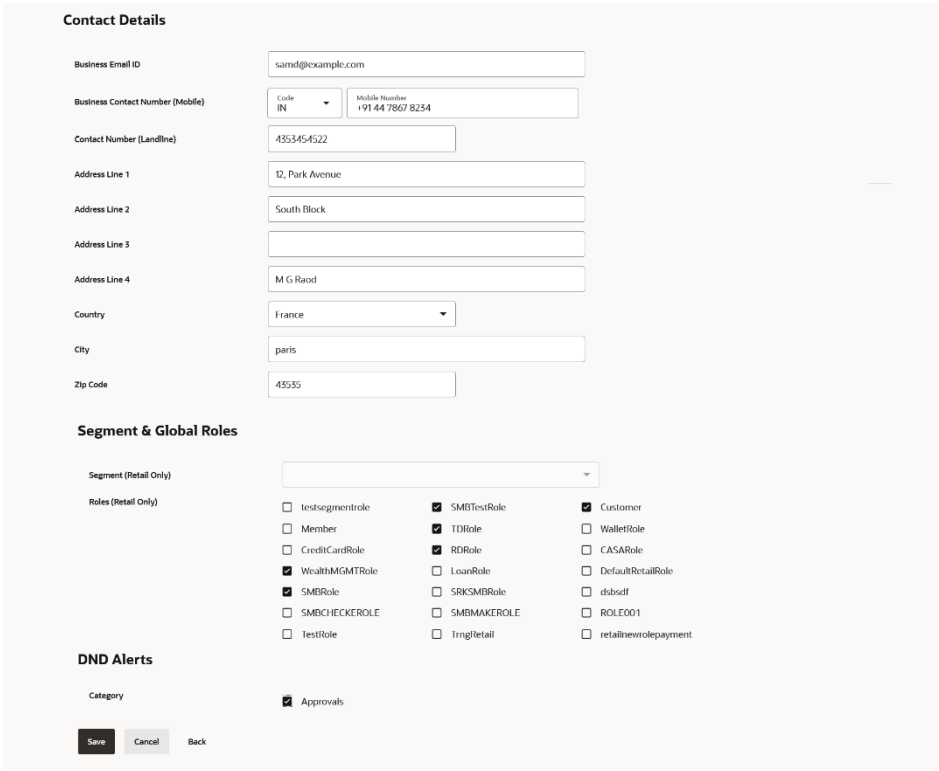
Note: In case of multi entity implementation, if the system/bank administrator has access to multiple entities, then the administrator can select the entity from the entity switcher on which the user needs to be on boarded. The selected entity of the user as part of onboarding will be the default/home entity of the user being created.

To create a new user:

1. In the **User Management** screen, click **Create**. The **User Management - Create New User** screen appears.
2. In the **User Management – Create New User** screen, do the following:
3. From the **User Type** list, select the appropriate type for the user being created.
   a. If you select the **Retail & Business User** option from the **User Type** list, the username needs to be provided;
      i. In the **User Name** field, enter the required details. Click **Check Availability** to check the uniqueness of the username.
      If the user ID is already used, then enter a unique valid username. The Entity, Party Details, **Personal Information, Contact Details, Limit & Roles, Touch Points** sections are also available .

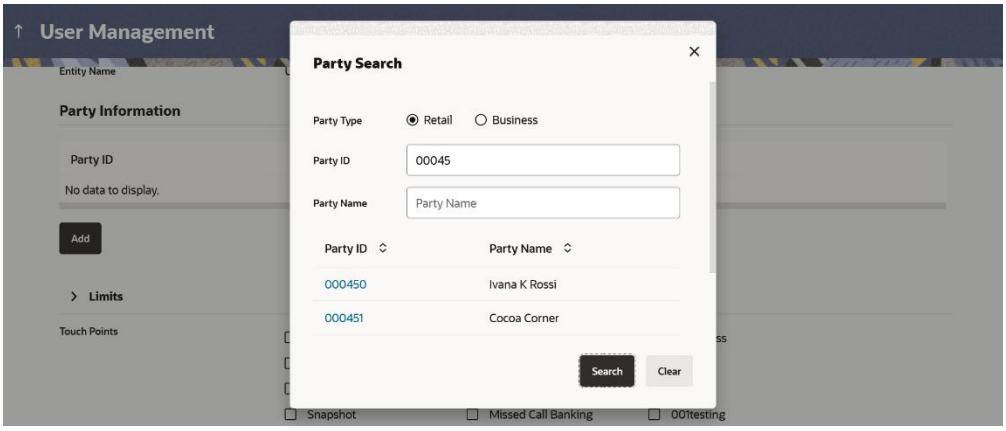
Create Retail & Business User





b. One Retail and multiple Business parties can be mapped to a user under each entity. Within the Primary Entity, click **Add** to capture party details. The **Party Search** popup screen appears.

Party Search



i. In the **Party Type** field, specify if the type of party is Retail or Business. This is a mandatory input.

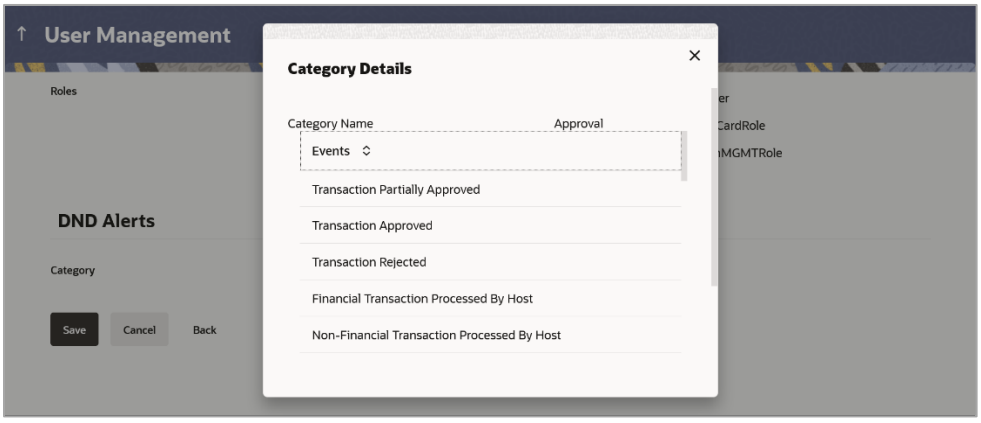
ii. In the **Party ID** field, enter the party ID.
OR
In the **Party Name** field, enter the party name partially or fully.

iii. Click **Search**.
In case of party ID search, the exact match appears if complete party ID is provided. In case of party name search, matching results are displayed if partial name is given.

Note: For all business parties, Party Preference maintenance is a must and business parties for which preferences are not maintained cannot be mapped to a user. Mapping corporate parties to a 'Retail & Business User' is not allowed.

iv. Select the **Party ID** from the search results.

DND Alerts - Category Details



Field Description

Field Name	Description
Create	
User Type	Type of user. The user can be: • Retail & Business User • Administrator
User Name	Name of the user.
Organization	Organization that the user belongs to. This field appears if you select **Administrator** option from **User Type** list.
Manager	Manager of the user. This field appears if you select **Administrator** option from **User Type** list.
Employee Number	Employee number of the user. This field appears if you select **Administrator** option from **User Type** list.
Primary Entity	
This section is applicable only for **Retail & Business** type of user.	
Party Information	
Click **Add** to add single or multiple parties under selected entity.	
Party ID	Party ID for which the user is to be created is displayed. This field appears if you select **Retail & Business** option from **User Type** list. **Note:** For Non Customer Corporates (counterparties on boarded by Corporates) the system will look for the party ID in OBSCF/OBCMS.
Party Name	Party Name of the party ID for which the user is to be created is displayed. This field appears if you select **Retail & Business** option from **User Type** list.

Field Name	Description
Party Type	Party type of the party ID for which the user is to be created is displayed. The party type can be Retail or Business.

Limit

This section appears if you select **Retail and Business User** option from the **User Type** list. If limit check is required, assign a limit package. In case of multi entity set up, limit packages need to be mapped at each entity level. All the touch points and touch point groups maintained in the system are listed under each entity. Packages can be mapped for each touch point and for a group. Also an option is provided to map the limit package at Global level (a system created group with all internal and external touch points). For business party transactions, a limit package maintained at the party level (as a part of party preference) will be considered and will be utilized.

Touch Points/ Group	Name of touch points/ groups under a specific entity to which the limit packages are to be mapped.
Package	List of the packages which can be mapped to touch points/ groups. Only limit packages maintained for the selected touch point/group will get listed here.
Actions	Indicates the option to reset the limit package assigned to the touch point/group. This can be achieved by clicking .
User Segment	Segment of the user for which the application role is created. All the application roles linked to the segment will get assigned to the user. This field appears for **Retail and Business** user type. Note: User can click on icon, which displays the roles linked to the selected user segment. All the roles associated to the segment gets assigned to the user.
Roles	Name of the application role. All the roles which are not associated to any User Segment gets displayed here. Administrator can assign additional roles (over and above to the roles assigned in segment).

Touch Points

Field Name	Description
Select Touch Points	The touch points (banking channels) allows a user to perform transactions using the touch points. The touch points could be: • Mobile Application • Mobile (Responsive) • Internet • Missed Call Banking • SMS Banking • Wearables • Snapshot • Siri / Chatbot • API Access • Soft Token Application

Accessible Entity Details

This section will only appear if the Bank has multi entity setup.

This section is applicable only for **Retail & Business** type of user.

Entity Name	Select the entity name i.e. accessible entity to be attached to the new user. This is applicable only if the Bank has a multi entity setup and the System/Bank administrator has access to more than one entity.
Touch Points/ Group	Name of touch points/ groups under a specific entity to which the limit packages are to be mapped.
Roles (Retails Only)	Name of the application role.

Personal Information

This section is applicable only for **Retail & Business** and **Administrator** type of user.

User Name	Define the name of the user (login ID) which is to be created. It is case insensitive. Note: Usernames are case insensitive i.e. User can login in OBDX with any case.

Field Name	Description
Title	Title of the user. If User type is **Retail and Business**, value is fetched from the core banking application and defaulted. For the user type corporate user and administrator are: • Mr • Mrs • Miss • Ms • Dr • Master
First Name	First name of the user. If user type is **Retail and Business User** , value is fetched from the core banking application and defaulted.
Middle Name	Middle name of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Last Name	Last name / surname of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Date of Birth	Date of birth of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Contact Details	
This section is applicable only for **Retail & Business** and **Administrator** type of user.	
Business Email ID	Email ID of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Email ID	Email ID of the user. This field is enabled for the **Administrator** type user.

Field Name	Description
Business Contact Number (Mobile)	Displays contact number of the user alongwith an international subscriber dialing (ISD) code. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Contact Number (Mobile)	The mobile number of the user alongwith an international subscriber dialing (ISD) code. This field is enabled for the **Retail and Business User** type user. Note: The mobile number field allow to capture the correct number of digits based on the selected country code.
Contact Number (Land Line)	Phone number (land line) number of the user.
Address Line 1-4	Address of the user. If user type is **Retail and Business User**, value is fetched from the host and defaulted value is fetched from the core banking application and defaulted.
Country	Country of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
City	City in which the user resides. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Zip Code	The postal code of the city in which the user resided. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Segment & Global Roles	
This section is applicable only for **Retail** type of user.	
Segment	Specify the segment to assign the role to it.
Global Roles	The global roles are available for mapping it to the users.

Field Name	Description
Roles	Application roles mapped to the user. In case of multi entity setup, these roles will be for the default/home entity of the user.

Global Roles

This section is applicable only for **Administrator** type of user.

Roles	The global roles are available for mapping it to the users.

DND Alerts

This section is applicable only for **Retail & Business** and **Administrator** type of user.

Category	Select the categories for which DND needs to be enabled. All the categories for which DND is applicable are available for selection. Note: Click on category link to view list of all the events for which alerts will not be sent to the user.

v. In the **Limits** section, select the limit packages to be mapped to touch points from the limit package list.

vi. Add the accessible entities for the user and select the party and limits for that entity (applicable only if Bank has Multi Entity setup), as follows:

1. Click **Add Accessible Entity** button, to add accessible entity to a user.
2. From the **Entity Name** list, select the name of the entity.
3. In the **Party ID** field, enter the party ID.
4. In the **Party Name** field, enter the party name.
5. Click **Search**. The search result is displayed.
6. Select the appropriate party ID.
7. In the **Limits** section, select the appropriate limit package under the **Package** for each touch point.

vii. From the **User Segment** list, select the appropriate segment for the user in **Limits and Roles** section. This field is present if a **Retail and Business** user type is being onboarded.

viii. Select the checkbox (s) against the **Roles,** to map to the selected **User Segment**.

ix. In the **Touch Points** section, select the check boxes beside the touch points to be mapped to the user.

x. In the **Personal Information** section, enter the required details.

xi. In the **Contact Details** section, enter the required details.

xii. From the **Segment** drop-down list under the **Segment & Global Roles** section, select the segment to assigned the role to it.

xiii. In the **Roles** field under the **Segment & Global Roles** section, select the checkbox (s) against the Roles, to map to the user.

xiv. In **Category** field under **DND Alerts** section, select the desired categories for which DND needs to be enabled.

b. If you select the **Administrator** option from the **User Type** list:

i. In the **User Name** field, enter the name of user which is to be created.

ii. Click **Onboard** to onboard the user. The required field to onborad the administrator populates.
OR
Click **Cancel** to cancel the transaction.
OR
Click **Clear** to reset the entered the details.

iii. In the **Organization** field, enter the organization of the employee.

iv. In the **Manager** field, enter the name of the manager of the user being created.

v. In the **Employee Number** field, enter the six digit employee number of the user.

vi. In the **Personal Information** section, enter the required details.

vii. In the **Contact Details** section, enter the required details.

viii. In **Category** field under **DND Alerts** section, select the desired categories for which DND needs to be enabled.

ix. In the **Touch Points** under **Primary Entity** section, select the check boxes beside the touch points to be mapped to the user.

x. Add the accessible entities for the user (applicable only if Bank has Multi Entity setup)

4. Click **Save** to save the user details.
OR
Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate to the previous screen.

5. The **Review** screen appears. Verify the details, and click **Confirm**.
OR
Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate to the previous screen.
The user will be navigated back to the create screen

6. The success message of user creation appears along with the transaction reference number.
Click **OK** to complete the transaction.

3.2 User Management - Search and View

Using this option, System/ bank administrators can search and view details of the existing users. Administrator selects the user type of the user to be searched.

System/ bank administrators can also change the user status or the channel access permission for a user using this screen.

Default search is available with Username, but the user can also be searched by providing other details like First Name, Last Name, Party ID. Email ID and Mobile Number.

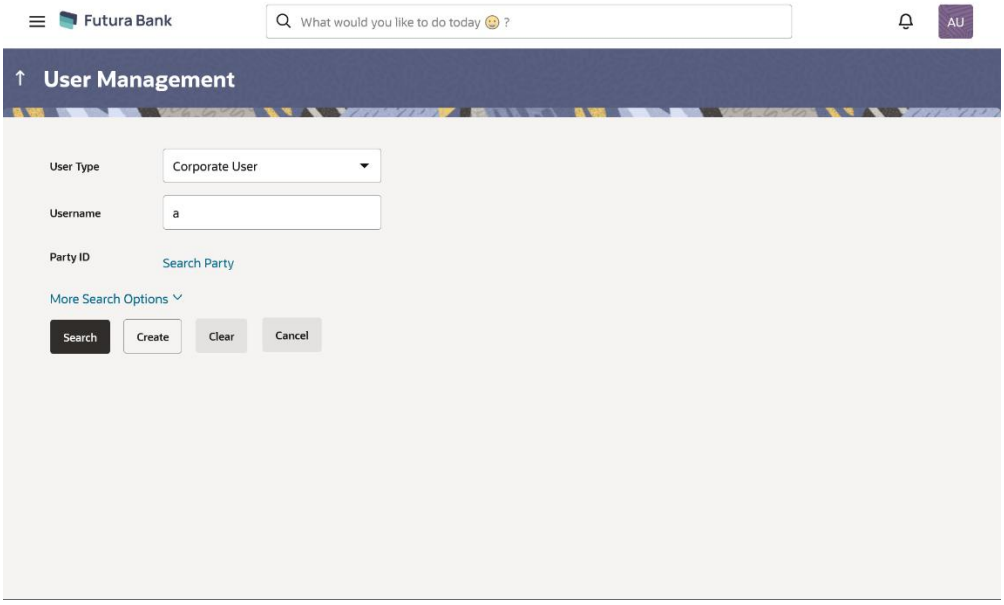
If the user type is selected as Retail & Business User, then the user can be searched based on the Party ID. An option is provided to search the party present in the core banking system using either the party ID or party name. The matching results are displayed on the screen.

If party ID or party name are provided partially, then a like search is run and all the records matching the search criteria are listed. If the complete party ID is entered, then the party ID is validated by the core banking application. After the core banking application validation is successful, party name gets displayed on the screen. In the result grid, the parties are listed with both Party ID and Party Name. User can select the record by clicking on the Party ID from the list.

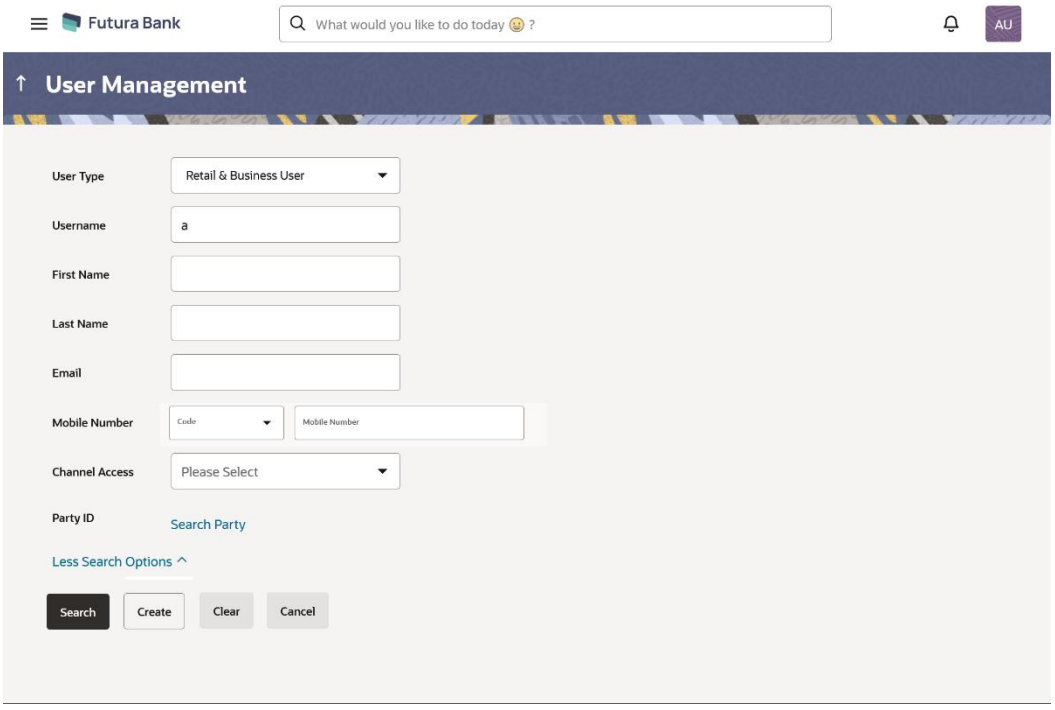
To search for a user:

1. Enter the search criteria, click **Search**.
   The search results appear on the **User Management** screen based on the search parameters.
   OR
   Click **Cancel** if you want to cancel the transaction.
   OR
   Click **Clear** if you want to reset the search parameters.

User Management - Search



User Management - More Search Options



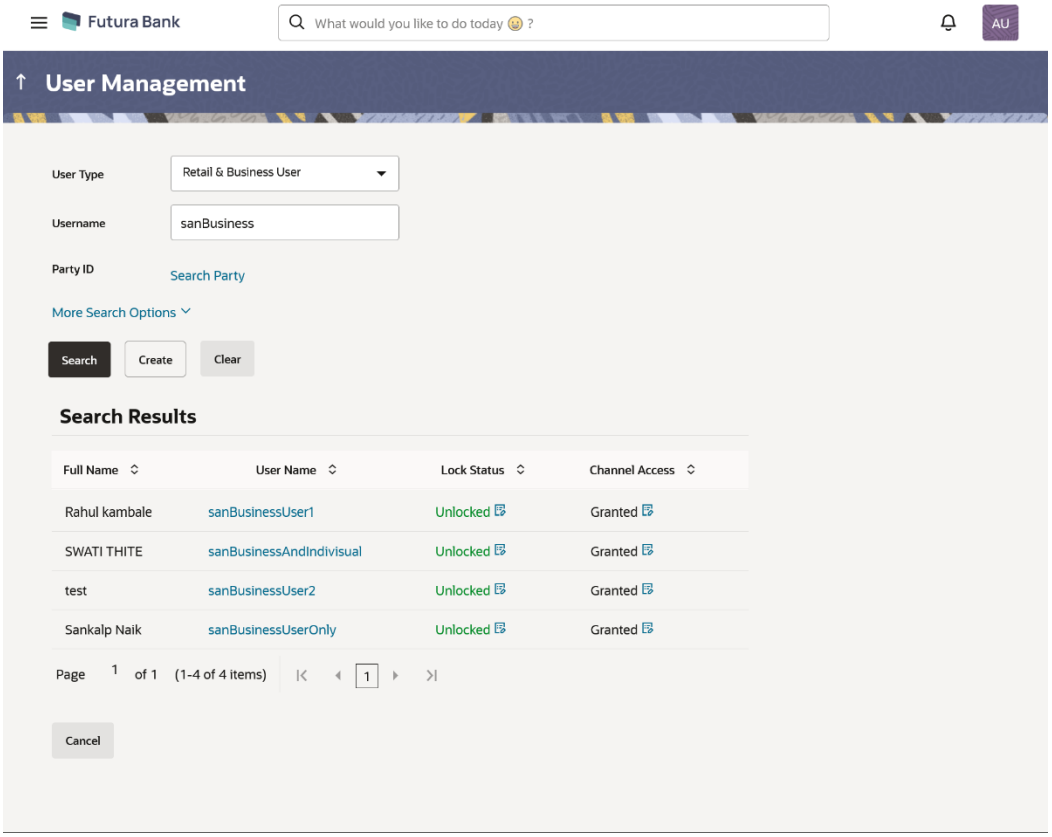
Field Description

Field Name	Description
User Type	Type of user to be searched. The user can be: • Corporate User • Administrator • Retail & Business User
User Name	To search the user with the user name. Partial search is allowed. The User ID is case insensitive.
More Search Options	
Below fields appears if you click the **More Search Options** link.	
First Name	Allows to search based on first name or given name of the user.
Last Name	Allows to search based on last name/ surname of the user.
Email	Allows to search based on email id of the user.
Mobile Number	Allows to search based on mobile number of the user. Note: User can select international subscriber dialing (ISD) code (country code) while selecting mobile number.
Channel Access	Allows to search based on channel access of the user.
Party ID	Allows to search based on Party id. This field appears if you select **Retail & Business or Corporate User** option from **User Type** list.

To view the user details:

1. Enter the search criteria and click **Search** in the **User Management** screen.
   The search results appear based on the search parameters.

User Management - Search Results



Field Description

Field Name	Description
Search Results	
Full Name	First name and last name of the user.
User Name	User Name of the user.
Status	Status of the user. Locked or Unlocked.
Channel Access	Indicates whether channel access is granted. Click to grant / revoke access rights. **Note**: Channel access feature is available for internal users only.

2. Click the **User Name** link of the record for which you want to view the user details. The **User Management - View** screen appears.

User Management - View

Field Description

Field Name	Description
View	

Field Name	Description
User Type	Type of user. The user can be: • Corporate User • Retail & Business User • Administrator
User Name	The name of the user. This field appears if you select **Retail & Business** option from **User Type** list.
Group Corporate ID	The group corporate ID mapped to the user is displayed. This field appears if you select **Corporate User** option from **User Type** list.
Party ID	The party ID mapped to the user is displayed. This field appears if you select **Retail & Business or Corporate User** option from **User Type** list.
Primary Entity	
Party Information	
Party ID	Displays the party ID mapped to the user. This field appears if you select **Retail & Business or Corporate User** option from **User Type** list. **Note:** For Non Customer Corporates (counterparties on boarded by Corporates) the system will look for the party ID in OBSCF/OBCMS.
Party Name	Displays the Party Name of the party ID mapped to the user. This field appears if you select **Retail & Business** option from **User Type** list.
Party Type	Displays the Party type of the party ID. The party type can be Retail or Business.

Field Name	Description
Organization	Organization that the user belongs to. This field appears if you select **Administrator** option from **User Type** list.
Manager	Manager of the user. This field appears if you select **Administrator** option from **User Type** list.
Employee Number	Employee number of the user. This field appears if you select **Administrator** option from **User Type** list.

Party Information

This section is displayed if you select **Retail & Business** option from **User Type** list.

Party ID	The party ID mapped to the user is displayed.
Party Name	Party Name of the party ID mapped to the user.
Party Type	Party type of the party ID mapped to the user.

Limit

This field appears if you select **Retail & Business** or **Corporate User** option from **User Type** list.

In case of multi entity setup, if the user has access to multiple entities, the limits package displayed will be the one associated to the default/home entity of the user. For business party transactions, a limit package maintained at the party level (as a part of party preference) will be considered and will be utilized.

Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for whom the limit packages are mapped.
Package	Name of the limit package mapped against specific touch points /touch point groups
Selected Segment	Segment of the user for which the application role is created. This field is displayed only for a **Retail & Business** user type.
Roles	Application roles mapped to the user. In case of multi entity setup, these roles will be for the default/home entity of the user.

Touch Points

Field Name	Description
Selected Touch Points	The touch points (banking channels) selected for a user to perform transactions. The touch points could be: • Mobile Application • Mobile (Responsive) • Internet • Missed Call Banking • SMS Banking • Wearables • Snapshot • Siri / Chatbot • API Access • Soft Token Application
Limits & Roles	
User Groups	Displays the user groups that are assigned to the user. This field is displayed only for a corporate user type.
Personal Information	
This section is displayed if you select **Retail & Business** & **Administrator** option from **User Type** list.	
User Name	Name of the user (login ID) of the user.
Title	Title of the user. The options are: • Mr • Mrs • Miss • Ms • Dr • Master
First Name	First name of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.

Field Name	Description
Middle Name	Middle name of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Last Name	Last name/ surname of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Date of Birth	Date of birth of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.

Contact Details

This section is displayed if you select **Retail & Business** & **Administrator** option from **User Type** list.

Business Email ID	Email ID of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Email ID	Email ID of the user. This field is enabled for the **Administrator** type user.
Business Contact Number (Mobile)	Displays contact number of the user alongwith an international subscriber dialing (ISD) code. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Contact Number (Mobile)	Displays mobile number of the user alongwith an international subscriber dialing (ISD) code. This field is enabled for the **Retail and Business User** type user.
Contact Number (Land Line)	Phone number (land line) number of the user.
Address Line 1-4	Address of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Country	Country of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.

Field Name	Description
City	City in which the user resides. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Zip Code	The postal code of the city in which the user resided. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.

Segment & Global Roles

This section is applicable only for **Retail** type of user.

Segment	View the segment assigned to the Retail user.

User Groups And Global Roles

User Groups	The list of all user groups to which the selected user belongs. User Group is applicable only to Corporate Users and Administrators. Note: • This information is read-only and hence cannot be modified. • If a particular user needs to be removed from a user group, then the administrator must manually go to the particular user group screen and remove the user.
Roles	The global roles which are mapped to the users.

Device Registration

This section is applicable only for **Corporate** type of user.

Android Devices	This option shows if the user has registered Zig Bank application on any android devices/s. Enabling of the device happens when the user installs and registers on the app on the android device. Administrator cannot manually enable the device. If the Administrator deregisters the device, the user gets logged out from all the android devices and his alternate login gets disabled from all the android devices on which the user has installed the application.

Field Name	Description
iOS Devices	This option shows if the user has registered Zig Bank application on any iOS devices/s. Enabling of the device happens when the user installs and registers on the app on the iOS device. Administrator cannot manually enable the device. If the Administrator deregisters the device, the user gets logged out from all the iOS devices and his alternate login gets disabled from all the iOS devices on which the user has installed the application.

Push Notifications

This section is applicable only for **Corporate** type of user.

Android Devices	This option shows if the user has registered for push notifications for android devices. Enabling of the push notification is done by user himself and administrator cannot do the same. If the administrator disables this, the user will stop getting notifications as a pop-up message (push notification) on the user's registered mobile number.
iOS Devices	This option shows if the user has registered for push notifications for iOS devices. Enabling of the push notification is done by user himself and administrator cannot do the same. If the administrator disables this, the user will stop getting notifications as a pop-up message (push notification) on the user's registered mobile number. **Note:** To receive push notification user will have to allow the same on the device settings.

Primary Entity Details

Entity Name	Primary Entity name associated to the user.
Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for which the limit packages are mapped.
Roles	For the primary entity selected/ added, system will default the roles same as that of home entity of the user. The administrator cannot define separate roles for each of the entities.

Map Parties

This section is applicable only for **Corporate** type of user.

Primary Party	Primary Entity name associated to the user.

Field Name	Description
Accessible Parties	Accessible Entities associated to the user.
Limits	Limits attached to the user.
Touch Points	Name of touch points/ groups maintained under a specific entity for which the limit packages are mapped.
Map Roles	
DND Alerts	
DND Alerts	The list of categories for which DND is configured can be enabled or disabled using this option.

Accessible Entity Details

This section is applicable only to **Retail** or **Admin** user only.

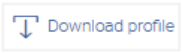
Entity Name	Accessible Entity name associated to the user.

Limits - Touch Point/Groups

Limits package associated to the user for the accessible entity. This field is only applicable for Retail & Business and corporate users. For Retail Party transactions, the limit package maintained at the user level will be considered and utilized. For business party transactions, a limit package maintained at the party level (as a part of party preference) will be considered and utilized.

Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for which the limit packages are mapped.
Package	Name of the limit package mapped against specific touch points /touch point groups.
Roles	For the accessible entity selected/ added, system will default the roles same as that of home entity of the user. The administrator cannot define separate roles for each of the entities.

3. Click **Edit** to edit the user details.
   OR
   Click **Reset Password** to reset user's password. For more information refer, **Reset password** section.
   If user clicks '**No**', the action gets cancelled.
   OR
   Click **Cancel** to cancel the transaction.
   OR

Click **Back** to navigate to the previous screen.
OR
Click  to download the user details.

1.

3.3 User Management - Edit

This function enables the Administrator to edit the existing user details.

Administrators will be allowed to modify the user details, including adding/removing parties mapped to the user. For a Retail & Business user, the primary entity should have at least 1 party mapped, however, if all the parties mapped under the linked entity are removed, then the entity access will also be removed from the user.

To edit or update user details:

1. Enter the search criteria, click **Search**.
   The search results appear on the **User Management** screen based on the search parameters.
   OR
   Click **Clear** if you want to reset the search parameters.
   OR
   Click **Cancel** if you want to cancel the transaction.
2. In the **User Management - Search Results** section, click the **User Name** link of the record for which you want to edit the user details.
   The **User Management - View** screen appears.
3. Click **Edit** to update the user information.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

User Management - Edit User

Field Description

Field Name	Description
Edit	
User Type	Type of user. The user can be: • Retail & Business User • Administrator
User Name	The name of the user. This field appears if you select **Retail & Business** option from **User Type** list.
Party ID	The party ID mapped to the user is displayed. This field appears if you select **Retail & Business** option from **User Type** list.
Primary Entity	
Party Information	
Party ID	Displays the party ID mapped to the user. This field appears if you select **Retail & Business or Corporate User** option from **User Type** list. **Note:** For Non Customer Corporates (counterparties on boarded by Corporates) the system will look for the party ID in OBSCF/OBCMS.
Party Name	Displays the Party Name of the party ID mapped to the user. This field appears if you select **Retail & Business** option from **User Type** list.
Party Type	Displays the Party type of the party ID. The party type can be Retail or Business.
Organization	Organization that the user belongs to. This field appears if you select **Administrator** option from **User Type** list.
Manager	Manager of the user. This field appears if you select **Administrator** option from **User Type** list.

Field Name	Description
Employee Number	Employee number of the user. This field appears if you select **Administrator** option from **User Type** list.
Primary Entity Details	
This section is applicable only to **Retail** or **Admin** user only.	
Entity Name	Primary Entity name associated to the user. This field is appears for **Retail** or **Admin** user only.
Party Information	
This section is displayed if you select **Retail & Business** option from **User Type** list.	
Party ID	The party ID mapped to the user is displayed.
Party Name	Party Name of the party ID mapped to the user.
Party Type	Party type of the party ID mapped to the user.
Limits	
This field appears if you select **Retail & Business** or **Corporate User** option from **User Type** list. In case of multi entity setup, if the user has access to multiple entities, the limits package displayed will be the one associated to the default/home entity of the user. For business party transactions, a limit package maintained at the party level (as a part of party preference) will be considered and will be utilized.	
Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for whom the limit packages are mapped. This field is appears for **Retail** or **Admin** user only.
Package	Name of the limit package mapped against specific touch points /touch point groups
Selected Segment	Segment of the user for which the application role is created. This field is displayed only for a **Retail & Business** user type.
Roles	Application roles mapped to the user. In case of multi entity setup, these roles will be for the default/home entity of the user. This field is appears for **Retail** or **Admin** user only.

Field Name	Description
Touch Points	
Selected Touch Points	The touch points (banking channels) selected for a user to perform transactions. The touch points could be: • Mobile Application • Mobile (Responsive) • Internet • Missed Call Banking • SMS Banking • Wearables • Snapshot • Siri / Chatbot • API Access • Soft Token Application
Accessible Entity Details	
This section is applicable only to **Retail** or **Admin** user only.	
Entity Name	Accessible Entity name associated to the user.
Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for whom the limit packages are mapped.
Roles	Application roles mapped to the user.
Personal Information	
This section is displayed if you select **Retail & Business** & **Administrator** option from **User Type** list.	
User Name	Name of the user (login ID) of the user.

Field Name	Description
Title	Title of the user. The options are: • Mr • Mrs • Miss • Ms • Dr • Master
First Name	First name of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Middle Name	Middle name of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Last Name	Last name/ surname of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Date of Birth	Date of birth of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Contact Details This section is displayed if you select **Retail & Business** & **Administrator** option from **User Type** list.	
Business Email ID	Email ID of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Email ID	Email ID of the user.This field is enabled for the **Administrator** type user.
Business Contact Number (Mobile)	Displays contact number of the user alongwith an international subscriber dialing (ISD) code. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.

Field Name	Description
Contact Number (Mobile)	Displays mobile number of the user alongwith an international subscriber dialing (ISD) code. This field is enabled for the **Retail and Business User** type user.
Contact Number (Land Line)	Phone number (land line) number of the user.
Address Line 1-4	Address of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Country	Country of the user. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
City	City in which the user resides. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Zip Code	The postal code of the city in which the user resided. If user type is **Retail and Business User**, value is fetched from the core banking application and defaulted.
Segment & Global Roles	
This section is applicable only for **Retail** type of user.	
Segment	View the segment assigned to the Retail user.
User Groups And Global Roles	
This section is applicable only for **Administrators** type of user.	
User Groups	The list of all user groups to which the selected user belongs. Note: • This information is read-only and hence cannot be modified. • If a particular user needs to be removed from a user group, then the administrator must manually go to the particular user group screen and remove the user.
Roles	The global roles which are mapped to the users.

Field Name	Description
Device Registration	
This section is applicable only for **Corporate** type of user.	
Android Devices	This option shows if the user has registered Zig Bank application on any android devices/s. Enabling of the device happens when the user installs and registers on the app on the android device. Administrator cannot manually enable the device. If the Administrator deregisters the device, the user gets logged out from all the android devices and his alternate login gets disabled from all the android devices on which the user has installed the application.
iOS Devices	This option shows if the user has registered Zig Bank application on any iOS devices/s. Enabling of the device happens when the user installs and registers on the app on the iOS device. Administrator cannot manually enable the device. If the Administrator deregisters the device, the user gets logged out from all the iOS devices and his alternate login gets disabled from all the iOS devices on which the user has installed the application.
Push Notifications	
This section is applicable only for **Corporate** type of user.	
Android Devices	This option shows if the user has registered for push notifications for android devices. Enabling of the push notification is done by user himself and administrator cannot do the same. If the administrator disables this, the user will stop getting notifications as a pop-up message (push notification) on the user's registered mobile number.
iOS Devices	This option shows if the user has registered for push notifications for iOS devices. Enabling of the push notification is done by user himself and administrator cannot do the same. If the administrator disables this, the user will stop getting notifications as a pop-up message (push notification) on the user's registered mobile number. **Note:** To receive push notification user will have to allow the same on the device settings.
DND Alerts	

Field Name	Description
DND Alerts	The list of categories for which DND is configured can be enabled or disabled using this option.

Limits - Touch Point/Groups

Limits package associated to the user for the accessible entity. This field is only applicable for Retail & Business and corporate users. For Retail Party transactions, the limit package maintained at the user level will be considered and utilized. For business party transactions, a limit package maintained at the party level (as a part of party preference) will be considered and utilized.

Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for which the limit packages are mapped.
Package	Name of the limit package mapped against specific touch points /touch point groups.
Roles	For the accessible entity selected/ added, system will default the roles same as that of home entity of the user. The administrator cannot define separate roles for each of the entities.

4. Update the required details.
5. Click **Save** to update the changes.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
6. The **Review User Details** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
7. The success message of updates appears.
   Click **OK** to complete the transaction.

.

FAQ

1. **Who can create / update the user?**

   System administrator, bank administrator and corporate administrator can create or edit the users. Corporate Administrator can create user for the party ID he belongs to.

2. **What type of combinations are allowed for the Retail & Business user type for the digital banking accesses ?**

   Users are provided with the following access combinations:

Relationships	Allowed/Not Allowed
One Retail	Allowed
Multiple Retail	Not Allowed
One Retail + One Business	Allowed
One Retail + Multiple Business	Allowed
Multiple Retail + Multiple Business	Not Allowed
One Business	Allowed
Multiple Business	Allowed

3. **Can I edit the party id mapped to the user?**

   No, party ID mapped to the user cannot be edited.

4. **When does the system update a user status as 'locked'?**

   User status can get locked if he has exceeded the maximum number of attempts allowed for entering a wrong password.

5. **When will the System/ Bank Administrator use Revoke Channel Access feature?**

Incase if the customer does not want to use his channel banking and requests bank to disable his internet banking, bank user can do the same by revoking the channel access for his user. Similarly if a corporate user leaves a corporate house, his channel access should be revoked using this feature, so that he should not be able to access the company accounts.

6. Can I set the user name which is already used in the application?

No, uniqueness of a user name/user ID is checked while creating or modifying a user.

7. Can I edit personal and contact details of Retail & Business user?

If any of the mapped party types is selected as 'Retail', the Personal, Contact and Address details of the user are fetched as read-only from the respective core banking application. If all the selected party/ies are 'Business' type, then the administrator is expected to fill the user's profile details manually..

8. Can one assign multiple Application roles to a user?

Yes, multiple Application roles can be assigned to the user. e.g. Corporate user is acting as maker of few transactions and approver of few other transactions.

9. What are the different roles available out of box?

Following are the Application role associated with each application role out of box.

User Type	Application Roles
Retail & Business User	**Customer**
Corporate User	• Maker • Checker • Viewer • Corporate Admin Maker • Corporate Admin Checker • Non Customer Maker • Non Customer Checker • Non Customer Viewer • Non Customer Corp Admin Maker • Non Customer Corp Admin Checker
Administrator	• Admin Maker • Admin Checker

10. **If I update the limit package associated with a user, what will happen to the in-flight transactions?**

    Yes, new limit package can be mapped to a user. Limits get applied from an immediate effect if the effective date is less than or equal to current date. And if the effective date is future date, the limit package will be applied from the date available in the package.

11. **If I update the Application role associated to a user, what will happen to the in-flight transactions?**

    In case of any update of Application roles mapped to the user as edit user functionality, the privileges associated with new child roles get applied to the user with an immediate effect. So if any transaction is pending with approver for approval, user can view and approve those transactions only if checker role is mapped to him. As soon as checker role is unmapped, then user will not be able to view and approve the transactions which were pending for his approval.

12. **Can administrator with one entity have right to create users in different entity?**

    No, administrator can only create users in his own entity only.

13. **Can I assign a user Segment to a Corporate User?**

    No, User Segment can only be attached to a Retail & Business type of user. However, segments are only applicable to Retail users.

14. **Can I assign additional roles to a Retail and Business user associated to a Segment?**

    Yes, system displays all the application roles which are not linked to a segment against the roles field, these roles can be attached to a user in addition to the roles attached to a segment.

15. **If a user's User ID is locked and he/she has requested for a reset password, does the admin needs to unlock it separately ?**

    No, the user ID will automatically get unlocked at the time of resetting the password by Admin.

4. Party Preferences

Party Preference setup allows the administrator to onboard the party on OBDX along with definition of attributes like limits, Approval flow, grace period etc. This maintenance is done for business as well as for corporate type of parties.

Separate limits will be applicable for the transaction done by each Retail & Business party. For Business Party transactions, the limit package maintained at the party level (as a part of party preference) shall be considered and utilized.

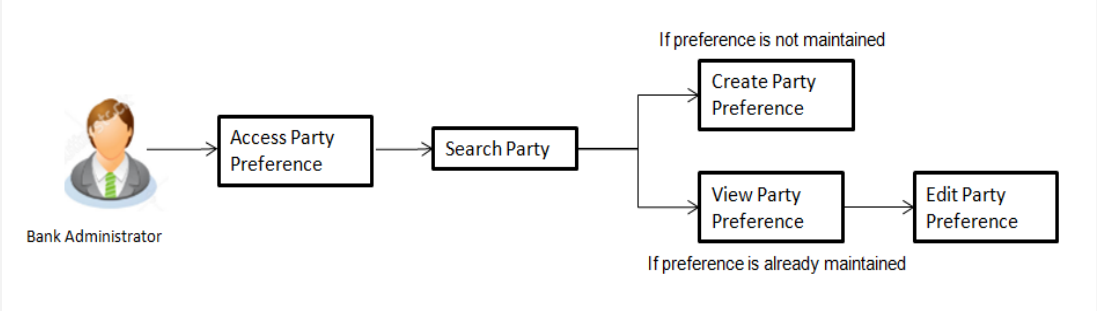
Parameter values maintained against a Corporate/Business party defines the system behavior for the following:

- Cumulative daily limits per transaction for the corporate party
- Transaction limits for the users
- Type of approval flow applicable
- Group Corporate Mapping
- Channel access preferences
- Availability of corporate administrator facility

Pre-Requisites

- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.
- Party for which preference needs to be set up is created in core banking application.

Workflow



Features Supported In Application

Party Preference maintenance features available for bank administrator in the application includes:

- Create Party Preferences
- View Party Preferences
- Edit Party Preferences

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu> Menu > Corporate Onboarding > Party Preferences
OR
Bank Administrator Dashboard > Corporate Onboarding > Party Preferences

Note: For Non Customer Corporates (for which the party id is not maintained in UBS or in Core banking system), can also be on boarded on OBDX using Party Preference. For such cases i.e. for non customer corporate (counterparties on boarded by Corporates) the system will look for the party ID in OBSCF/OBCMS.

4.1 Party Preferences- Search

Bank Administrator logs into the system and navigates to the Party Preferences screen.

System displays a screen to enter the party information (party ID or party name) and search party for which the preferences are to be maintained or viewed.

User can enter the party ID (if known) or the party name with a minimum of 5 characters. System matches the input provided by the user with the party name records and displays the matching party records.

In case of a party search by party ID, it is an exact match and system displays the party preference maintained if any, else displays an option to create party preference.

In case of a party search by account type and account number, system displays the associated party ID and Party name in the search results. The records have parties listed with both Party ID and Party Name information. User can select the record by clicking on the Party ID from the list.

To search party preferences of party:

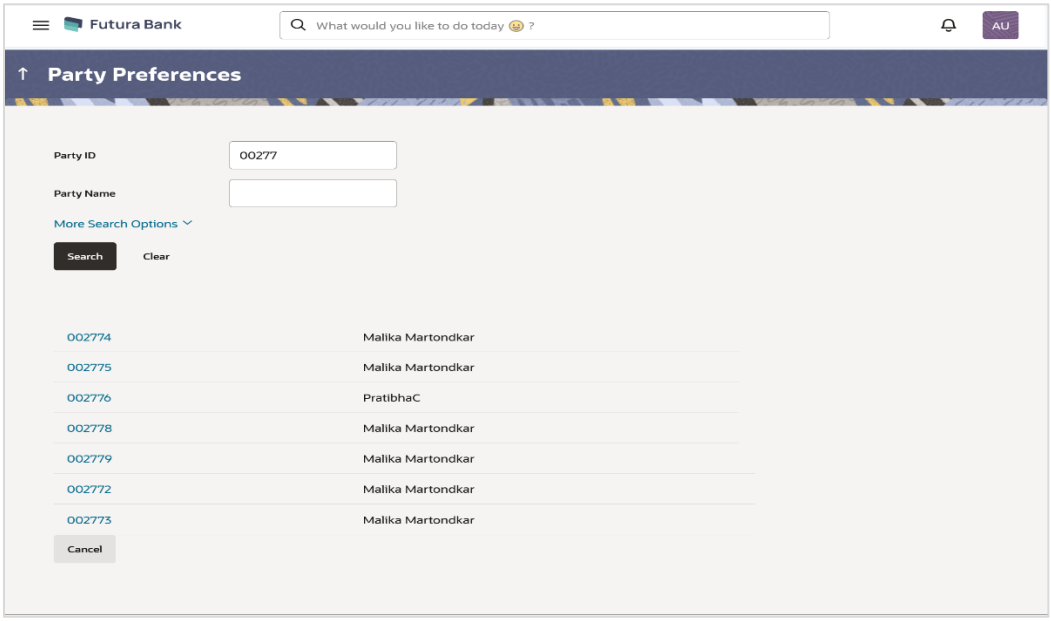
1. In the **Party ID** field, enter the party ID whose party preferences you want to view.
   OR
   In the **Party Name** field, enter the name of the party whose party preferences you want to view.

   OR

   In the **Account Type** field, select account type (i.e. CASA,TD & Loan) and Enter account number of party whose party preferences you want to view

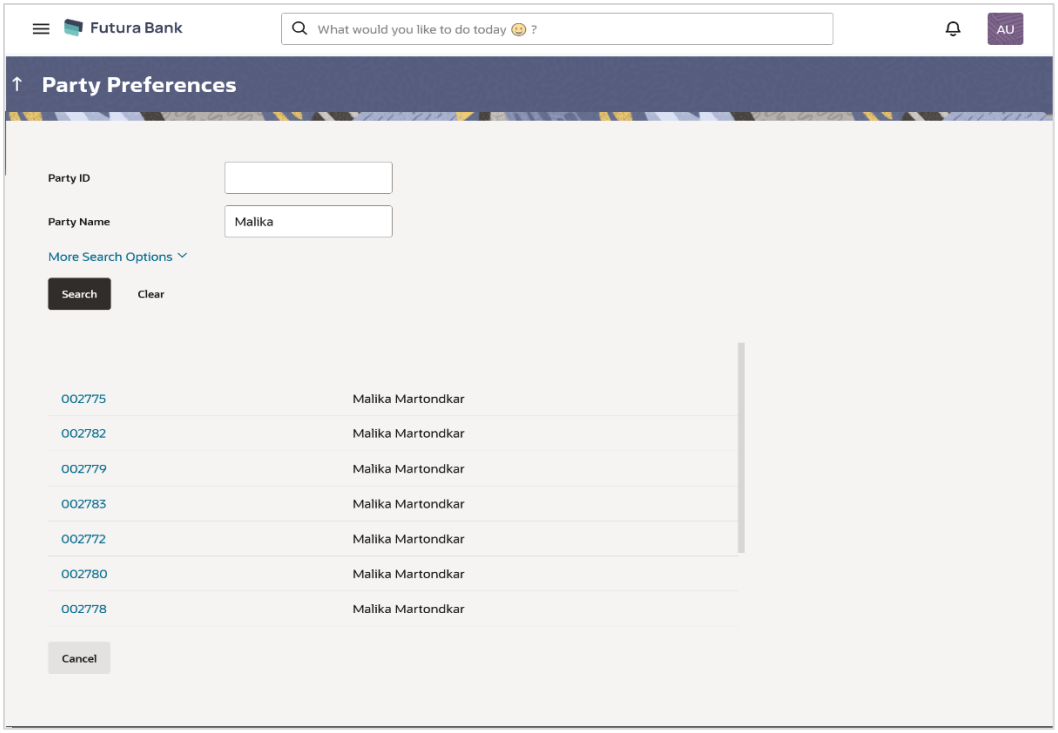
2. Click **Search**.
   If party preference is already maintained, user is directed to **Party Preference – View** screen.
   If party preference is not maintained, user is directed to **Party Preference – Create** screen.
   In case of invalid party, error message is shown on the screen.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.

Party Preferences- Search (Party ID)

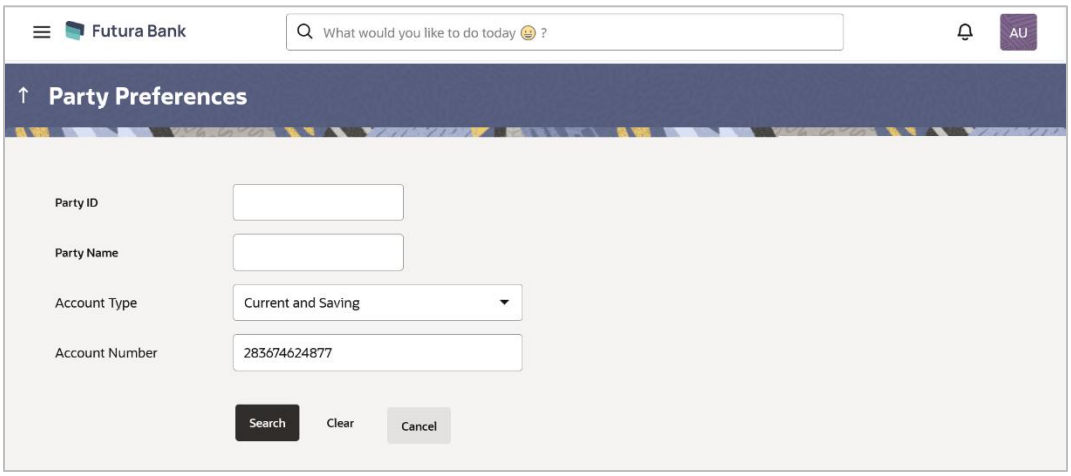


In case of a party search by name, system displays the matching party records. The records have parties listed with both Party ID and Party Name information. User can select the record by clicking on the Party ID from the list.

Party Preferences- Search (Party Name)



Party Preferences- Search(Account Number & Account Type)



Field Description

Field Name	Description
Search	
Party ID	Party ID for which the party preference to be maintained/ viewed.
Party Name	Party Name of a party for which the party preference to be maintained or viewed.
Account Type	Account type of Party for which the party preference to be maintained/ viewed. Account type can either CASA, TD, Credit Card & Loan.
Account Name	Account Number of a party for which the party preference to be maintained or viewed.

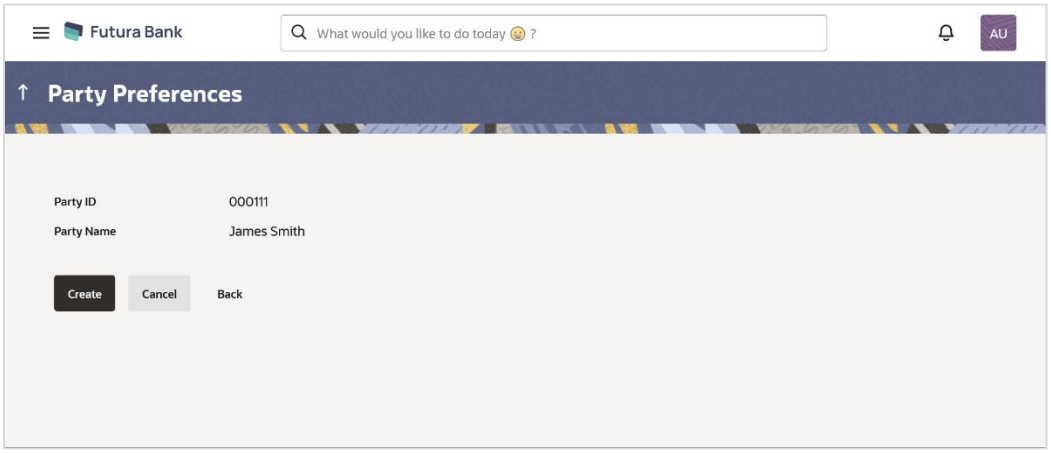
4.2 Party Preferences - Create

Using this option, Bank Administrator can configure party preferences for a specific party.

To create the party preferences:

1. In the **Party ID** field, enter the party ID for which you want to view the party preferences. Party ID entered by the user gets validated from the core banking application. After the core banking application validation is successful, a check is performed in application to verify if preferences are already maintained for a party.
   If the preferences are already maintained then user is directed to **Party Preference – View** screen.
   If party preference is not maintained, user is directed to **Party Preference – Create** screen.
   In case of invalid party, error message is shown on the screen.
2. Click **Search**.
   The party preference maintained for the party ID appears based on the entered search parameters.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
3. Click the desired party ID link under the **Party ID** column.
   The **Party Preferences** screen appears.

Party Preferences



Field Description

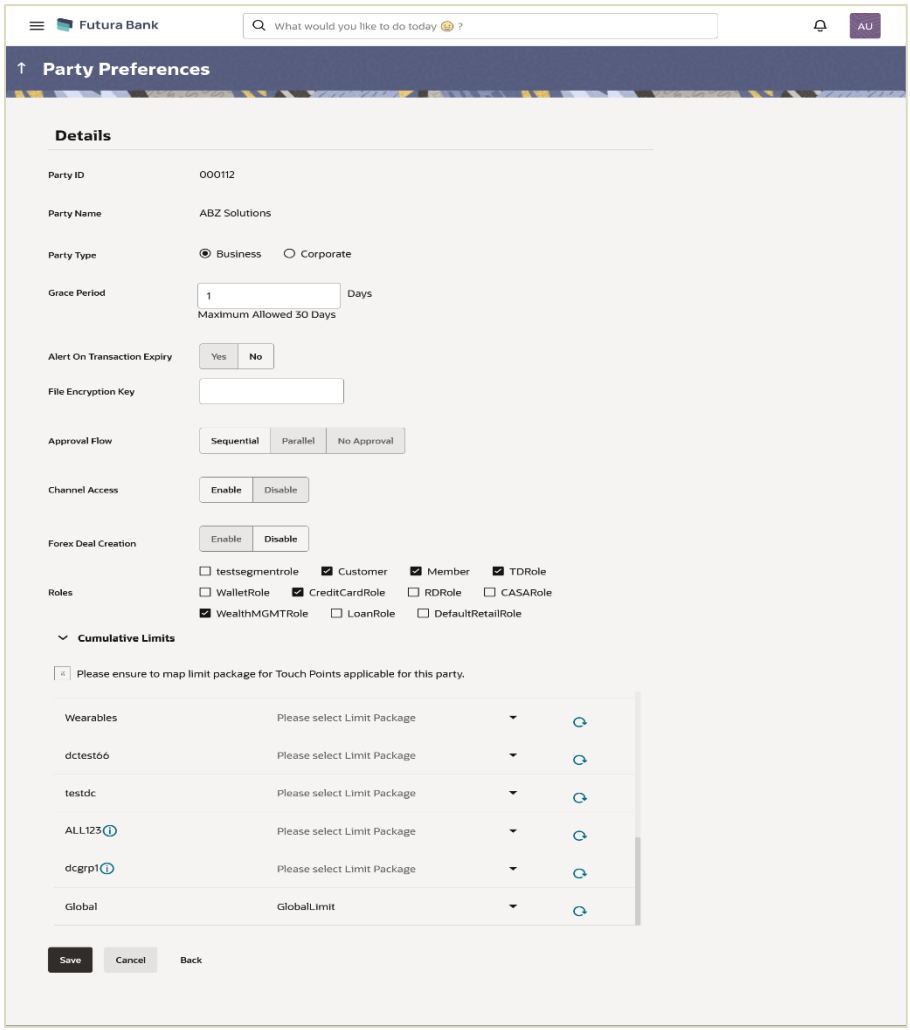
Field Name	Description
Search	
Party ID	Party ID for which the party preference to be maintained or viewed

Field Name	Description
Party Name	Name of a party for which the party preference to be maintained/ viewed.

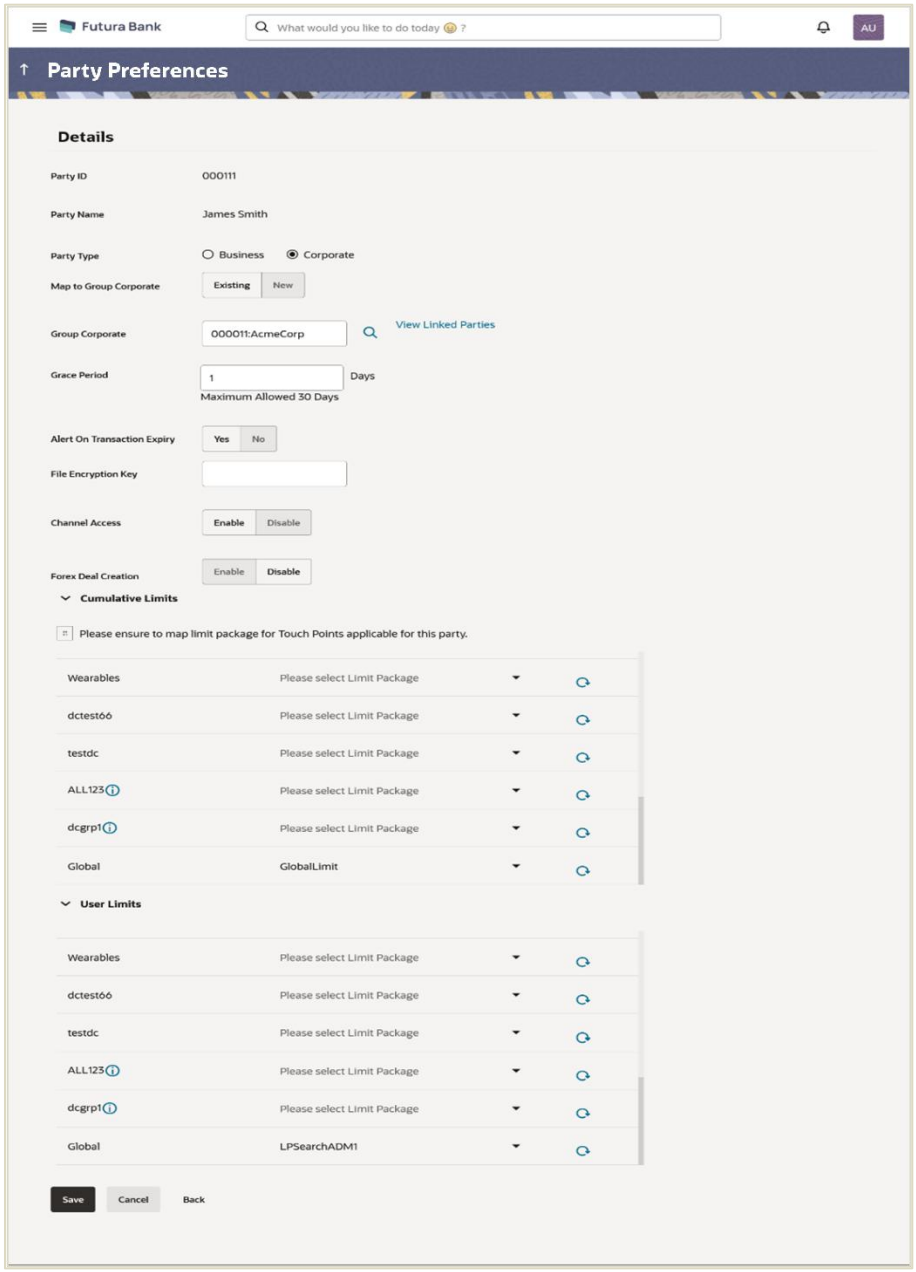
4. Click **Create** to create party preference.
   The **Create** screen appears.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction.
5. In the **Party Type** field, select the party type for which party preference is to be maintained.

Note: When the party type is selected as 'Corporate', the fields relevant to Group Corporate are shown. The fields applicable for Business user will not be shown if 'Business' party type is selected.

Party Preferences Maintenance – Create (Business Party)



Party Preferences Maintenance – Create (Corporate Party)



Field Description

Field Name	Description
Create	
Party ID	Party ID for which the party preference to be maintained.

Field Name	Description
	Note: For Non Customer Corporates (counterparties on boarded by Corporates) the system will look for the party ID in OBSCF/OBCMS.
Party Name	Party Name of a party for which the party preference to be maintained.
Party Type	Party type for which the party preference is to be maintained. The type can be: • Business • Corporate
Map to Group Corporate	Select this to map corporate party to Group Corporate. Note : • **Existing** – Click this to map with existing Group Corporate maintained within system • **New** –Click this to map corporate party with new Group Corporate Note: This field is enabled if **Corporate** is selected in **Party Type** field.
Group Corporate	Group Corporate ID and Name with which the Corporate Party is to be mapped. Note: This field is enabled if **Corporate** is selected in **Party Type** field.
View Linked Parties	If an existing Group Corporate is selected, a link is available to view the linked parties. Click on the link to view the linked parties under a Group Corporate. Note: This field is enabled if **Corporate** is selected in **Party Type** field.
Grace Period	Provision of time period is made to allow user to approve the transaction after the actual due date. **Note:** The tooltip with information will appear on dashboard in the **Pending for Approvals** section only when the user hovers on grace period.

Field Name	Description
Grace Period Expiry Alert	Enter the number of days prior to Grace Period Expiry, before which the alert needs to be sent to Maker and Approver regarding transaction approval expiry period. For e.g. if the value is set as 1 in this field then the alert should be sent one day before the grace period expiry date. **Note:** 1) The value entered in this field should be less than the value entered in **Grace Period** field. 2) If there is no **Grace Period** present, then this field will not get enabled.
Occurrence	Specify the alert preference. The options are: • Recurring- an alert will be sent daily, starting from the number of days configured in the above field before the before the grace period expiry date till the transaction is approved or expired (whichever is earlier) . • One Time- an alert would be sent only once with respect to value set in Grace Period For eg. if the grace period is set as 5 days, and the days before the alert is required to be sent is set as 3 days and the alert preference is set as recurring then an alert will be sent for 3 days in a row (daily) before the grace period expiry date or until the transaction is approved (whichever is earlier) . if this parameter is set as 'one time' then the alert would be sent only once i.e. 3 days before the grace period expiry date. **Note:** 1) The field will become 'Mandatory' if the user inputs value in the **Grace Period Expiry Alert** field. 2) If there is no **Grace Period** present, then this field will not get enabled.
Alert on Transaction Expiry	Specify if the alert is required to be sent on the Transaction Expiry Date. The options are: • Yes • No

Field Name	Description
	Note: 1) The field will become 'Mandatory' if the user inputs value in the **Grace Period** days field. 2) If there is no **Grace Period** present, then this will not get enabled.
File Encryption Key	File Encryption key is the unique key provided to the corporate for encrypting/decrypting the bulk files that he is uploading. Note: This field is enabled if **Corporate** is selected in **Party Type** field.
Approval Flow	The approval type for the party. The options are: • Sequential • Parallel • No Approval
Channel Access	Whether users associated with a party can start transacting through the channel. The options are: • Enable : Allows bank administrator to enable the party for channel access • Disable: Allows bank administrator to disable the party for channel access
Forex Deal Creation	Whether users associated with a party can create forex deals. The options are: • Enable: If this option is enabled, corporate user associated with this party can create forex deals. • Disable: If this option is disabled, corporate user associated with this party cannot create forex deals.
Roles	Application roles mapped to the user. In case of multi entity setup, these roles will be for the default/home entity of the user. These roles are applicable only for a Business Party Type.
Cumulative Limit	
	Note: These limits are applicable for a **Business** and **Corporate** Party Type.

Field Name	Description
It allows Bank Administrator to map customer cumulative daily limits to the party. All the touch points and touch point groups maintained the system are listed on the screen. Administrator needs to ensure that the relevant packages are mapped to all the touch points/groups accessible by the party users. Also an option is provided to map the limit package at Global level (a group created with all internal and external touch points) All the touch points and touch point groups maintained in the system are listed under each entity. Packages can be mapped for each touch point and for a group. For Business Party transactions, the limit package maintained at the party level (as a part of party preference) shall be considered and utilized.	
Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for which the limit packages are to be mapped.
Package	List of the packages available for mapping to touch points/ group are listed here. Limit packages maintained for the selected touch point will get here.
Actions	Click to refresh the option.

User Limits

This field allows the Bank Administrator to map customer user level limits (CUL) to the party. All the touch points and touch point groups maintained the system are listed on the screen. Administrator needs to ensure that the relevant packages are mapped to all the touch points/groups accessible by the selected party users. Also an option is provided to map the limit package at Global level (a group created with all internal and external touch points).

Note: These limits are applicable only for a **Corporate Party** Type.

Touch Points/ Group	Name of touch points/group maintained under a specific entity for which the user limit packages are to be mapped.
Package	List of the packages available for mapping to touch points/ group are listed
Actions	Click to refresh the option.

a. If you select the **Business** option in the **Party Type** field;

   v. Follow the steps from 6.

b. If you select the **Corporate** option in the **Party Type** field

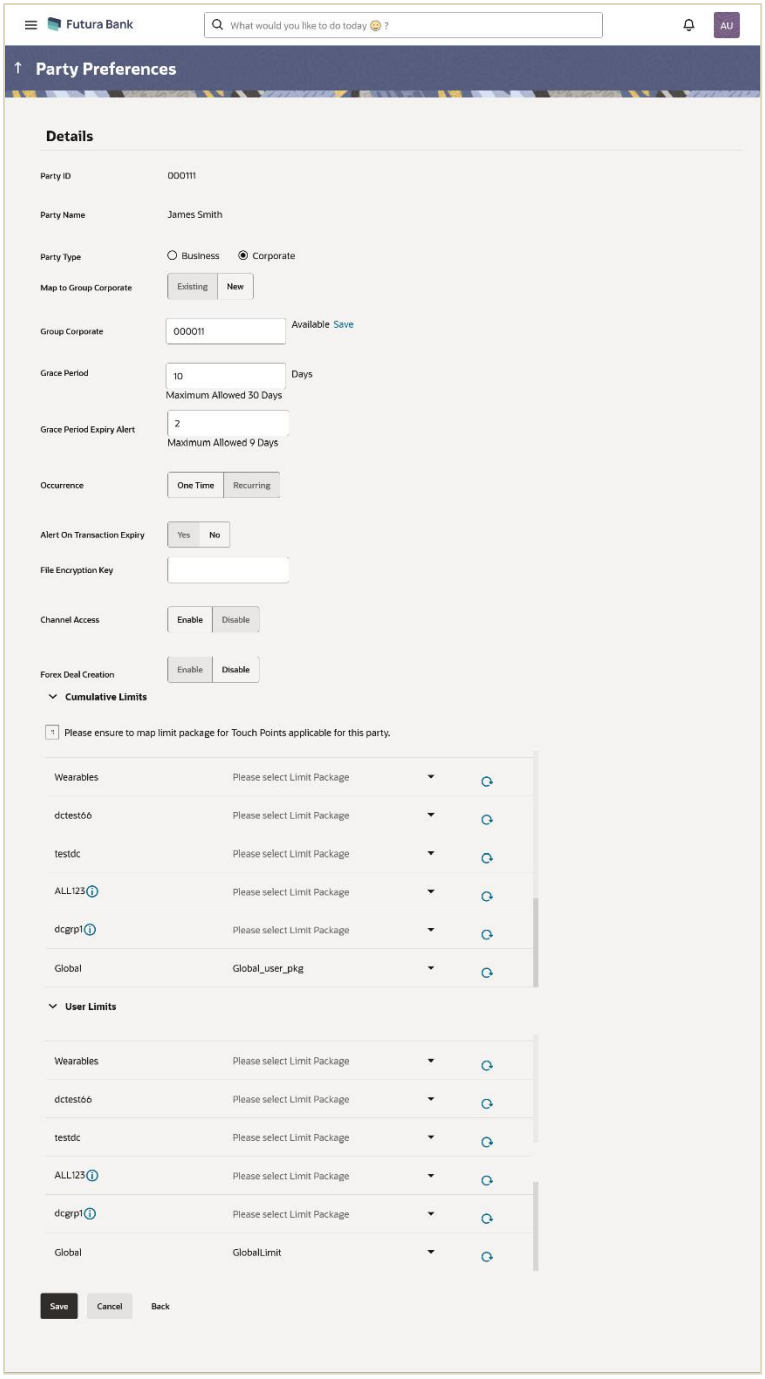
   Admin can map a party to an existing Group Corporate or can create a new Group Corporate by providing a new name:

   1. In the **Map to Group Corporate** field, select the option to map corporate party to Group Corporate.

i. If you select **New** option, the new Group Corporate is created and mapped to party,

Admin will provide a Group Corporate name and click on ‘check availability’ to check if the Group Corporate name entered is available in the application (as the name has to be unique). If the Group Corporate name is available, admin can click on save and system will show the Group corporate ID and name on the screen.

Corporate Party Map with New Group Corporate


Futura Bank
What would you like to do today ?
AU
Party Preferences
Details
Party ID
000111
Party Name
James Smith
Party Type
Business
Corporate
Map to Group Corporate
Existing
New
Group Corporate
00011
Available
Save
Grace Period
10
Days
Maximum Allowed 30 Days
Grace Period Expiry Alert
2
Maximum Allowed 9 Days
Occurrence
One Time
Recurring
Alert On Transaction Expiry
Yes
No
File Encryption Key
Channel Access
Enable
Disable
Forex Deal Creation
Enable
Disable
Cumulative Limits
Please ensure to map limit package for Touch Points applicable for this party.
Wearables
Please select Limit Package
dctest66
Please select Limit Package
testdc
Please select Limit Package
ALL123
Please select Limit Package
dcgrp1
Please select Limit Package
Global
Global_user_pkg
User Limits
Wearables
Please select Limit Package
dctest66
Please select Limit Package
testdc
Please select Limit Package
ALL123
Please select Limit Package
dcgrp1
Please select Limit Package
Global
GlobalLimit
Save
Cancel
Back

Field Description

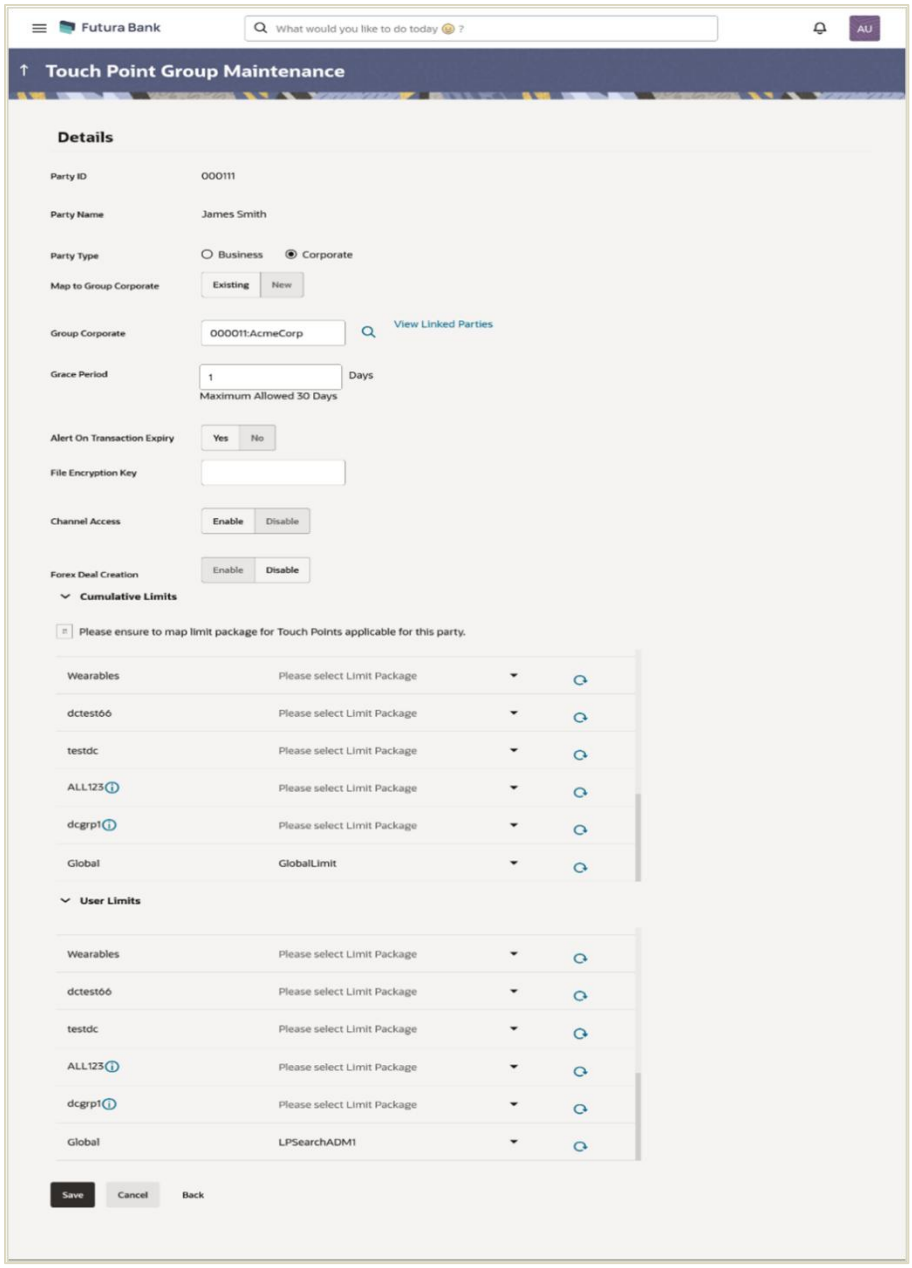
Field Name	Description
Search	
Group Corporate Name	Enter the new Group Corporate Name to map with the Corporate party whose preferences is being setup
Search Result	
Group Corporate ID	The Group Corporate ID will be fetched from the application and will be assigned to the new Group Corporate
Group Corporate Name	List of Corporate Name that can be mapped with the Corporate party

OR

If you select **Existing** option, the party is mapped to the existing Group Corporate,

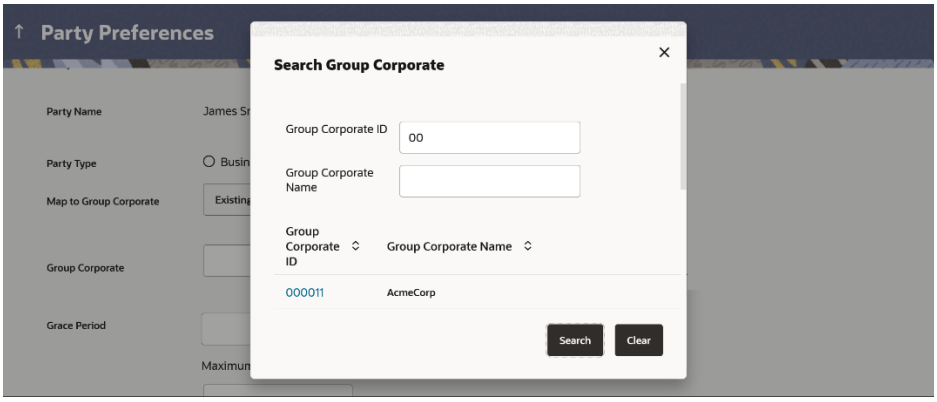
Admin can search an existing Group Corporate ID with the help of search panel provided to map with corporate party.

Corporate Party Map with Existing Group Corporate



1) In the **Group Corporate** field, enter the existing group corporate ID, and click on the icon. The **Search Group Corporate** popup appears.

Search Group Corporate to Map with Existing Group Corporate

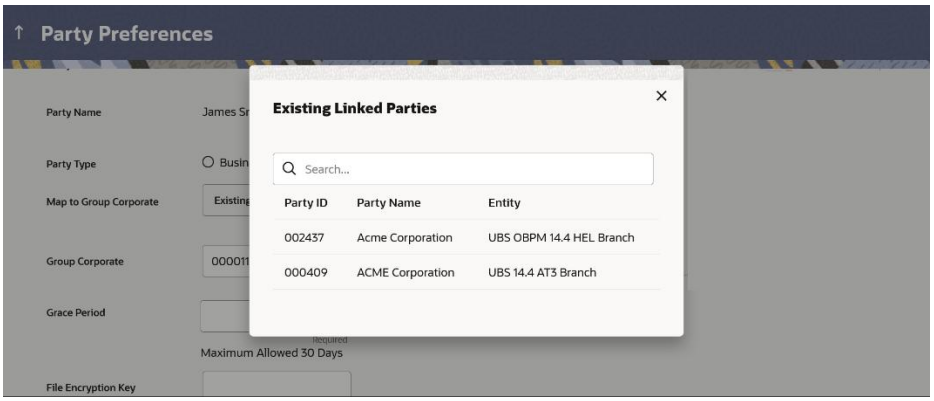


Field Description

Field Name	Description
Search	
Group Corporate ID	Search Group Corporate ID to map with the Corporate party whose preferences are being setup
Group Corporate Name	Search Group Corporate Name to map with the Corporate party whose preferences are being setup
Search Result	
Group Corporate ID	List of Group Corporate ID that can be mapped with the Corporate party
Group Corporate Name	List of Corporate Name that can be mapped with the Corporate party

2) Click on the **View Linked Parties** link to view the parties linked to selected Group Corporate.

View Linked Parties



6. **Note :** If Group **Corporate** flag is set as 'On' in system rules then,
   • It is mandatory to map a Group Corporate ID In Party Preferences
   • Even if it is a single party onboarding , it has to be mapped to a Group Corporate IDIn the **Grace Period** field, enter the number of grace period.
7. In the **Grace Period Alert** field, enter the days prior to Grace Period Expiry, to alert Maker and Approver regarding transaction approval expiry period.
8. In the **Occurrence** field, specify the alert preference.
9. In the **Alert On Transaction Expiry** field, specify whether to send alert on the transaction expiry date or not.
10. In the **File Encryption Key** field, enter the unique File Encryption key provided to the corporate for encrypting/decrypting the bulk files that he is uploading.

Note: This field is enabled if the **Corporate** option selected in **Party Type** field.

11. In the **Approval Flow** field, select the appropriate option.
12. In the **Channel Access** field, select the appropriate option.
13. In the **Forex Deal Creation** field, select the appropriate option.
14. Select the checkbox (s) against the **Roles**, to map to the selected party.

Note: **Roles** field is enabled only for Business type of party.

15. From the **Cumulative Daily Limits** list, select the appropriate option to map limit package for Touch Points applicable for this party.
16. From the **User Limit** list, select the appropriate option. These limits are applicable only to Corporate Party Type.

Note:

1) Click to refresh the option.
2) This field is enabled if the **Corporate** option selected in **Party Type** field.

17. Click to view the details of touch points group. The **View Details** popup window appears.

View Details- Touch Point Group

Field Description

Field Name	Description
Group Code	Group code defined for touch point group.
Group Description	Group description defined for touch point groups.
Touch Point / Group Type	Type of touch point i.e. whether touch point is of type internal or external.
Touch Points	List of the internal or external touch points.

18. Click **Save** to save party preferences.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to previous screen.
19. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.
20. The success message of party preference creation appears.
    Click **OK** to complete the transaction.

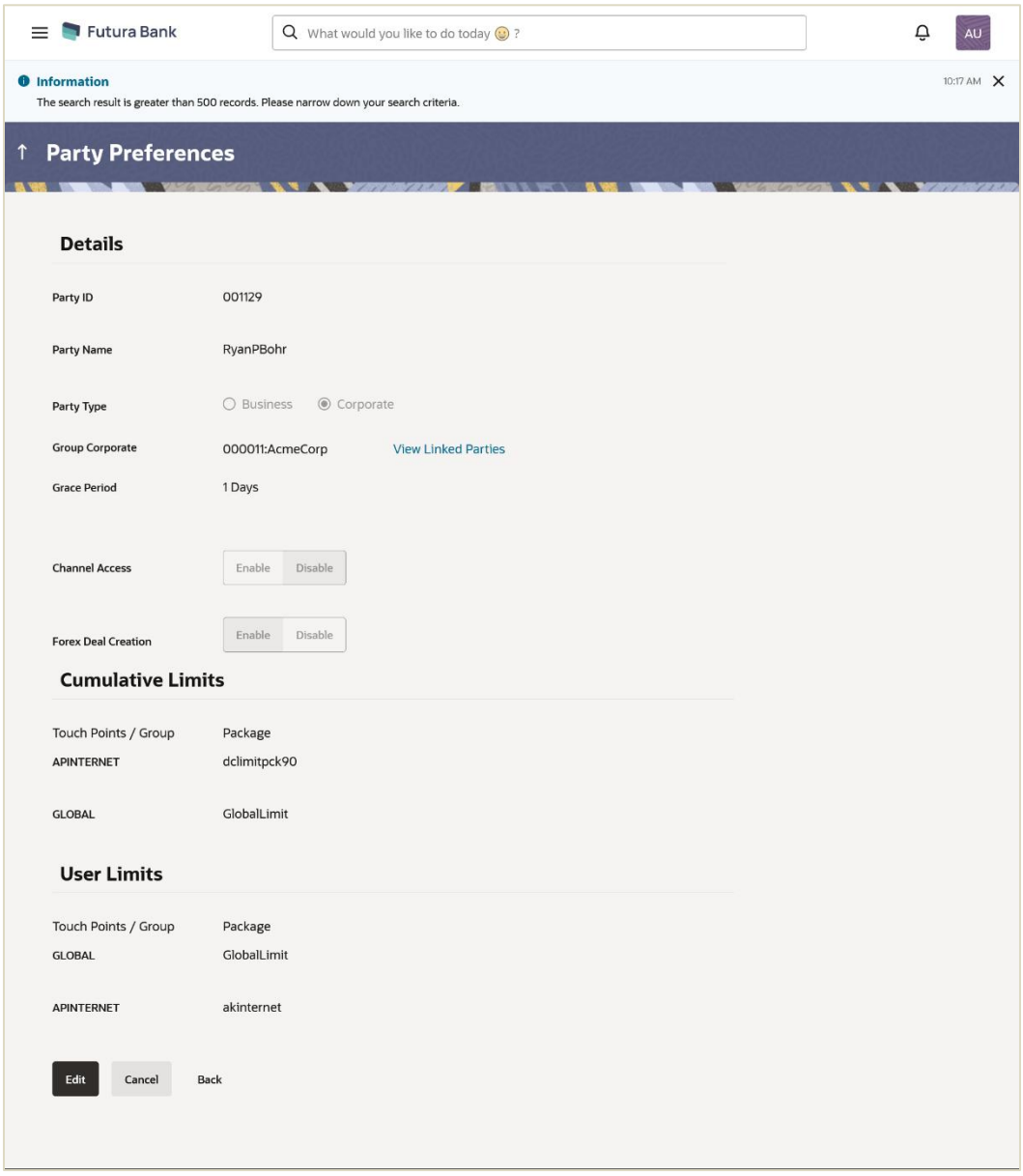
4.3 Party Preferences- View

Administrator user is directed to Party Preference – View screen if preference for the party is already maintained. Preferences set for the party will be displayed on the screen.

To view party preferences of party:

1. In the **Party ID** field, enter the party ID whose party preferences you want to view.
   OR
   In the **Party Name** field, enter the name of the party whose party preferences you want to view.
2. Click **Search**.
   The party preference maintained for the party ID appears based on the entered search parameters.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
3. Click the link under the **Party ID** column.
   The search result according to the search criteria appears.

Party Preferences- View



Field Description

Field Name	Description
Details	
Party ID	Party ID for which the party preference to be maintained.

Field Name	Description
Party Name	Party Name of a party for which the party preference to be maintained.
Party Type	Type of the party for which the party preference to be maintained.
Group Corporate	Group Corporate ID and Name with which the Corporate Party is mapped This field is enabled only for the **Corporate** party.
View Linked Parties	Click on the link to view the linked parties under the selected Group Corporate. This field is enabled only for the **Corporate** party.
Grace Period	Provision of time period is made to allow user to approve the transaction after the actual due date. **Note:** The tooltip with information will appear on dashboard in the **Pending_for_Approvals** section only when the user hovers on grace period.
Grace Period Expiry Alert	Displays the days prior to Grace Period Expiry to alert Maker and Approver regarding transaction approval expiry period.
Occurrence	Displays the alert preference set is recurring or needs to be sent once.
Alert on Transaction Expiry	Displays the alert is required to be sent on the transaction expiry date or not.
Approval Flow	The approval type for the party. The options are: • Sequential • Parallel • No Approval
Channel Access	Whether users associated with a party can start transacting through the channel. The options are: • Enable : Allows bank administrator to enable the party for channel access • Disable: Allows bank administrator to disable the party for channel access

Field Name	Description
Forex Deal Creation	Whether users associated with a party can create forex deals. The options are: • Enable: If this option is enabled, corporate user associated with this party can create forex deals. • Disable: If this option is disabled, corporate user associated with this party cannot create forex deals.
Roles	Application roles mapped to the user. In case of multi entity setup, these roles will be for the default/home entity of the user. These roles are applicable only for a Business Party Type.

Cumulative Limit

It allows Bank Administrator to map customer cumulative daily limits to the party. All the touch points and touch point groups maintained the system are listed on the screen. Administrator needs to ensure that the relevant packages are mapped to all the touch points/groups accessible by the party users. Also an option is provided to map the limit package at Global level (a group created with all internal and external touch points)

All the touch points and touch point groups maintained in the system are listed under each entity. Packages can be mapped for each touch point and for a group. For Business Party transactions, the limit package maintained at the party level (as a part of party preference) shall be considered and utilized.

Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for which the limit packages are to be mapped.
Package	List of the packages available for mapping to touch points/ group are listed here. Limit packages maintained for the selected touch point will get here.
Global	The global limits available for assigned to the party.

User Limits

This field allows the Bank Administrator to map customer user level limits (CUL) to the party. All the touch points and touch point groups maintained the system are listed on the screen. Administrator needs to ensure that the relevant packages are mapped to all the touch points/groups accessible by the selected party users. Also an option is provided to map the limit package at Global level (a group created with all internal and external touch points).

These limits are applicable only for a **Corporate** Party Type.

Touch Points/ Group	Name of touch points/group maintained under a specific entity for which the user limit packages are to be mapped.

Field Name	Description
Package	List of the packages available for mapping to touch points/ group are listed

4. Click **Edit** to edit the party preferences.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.

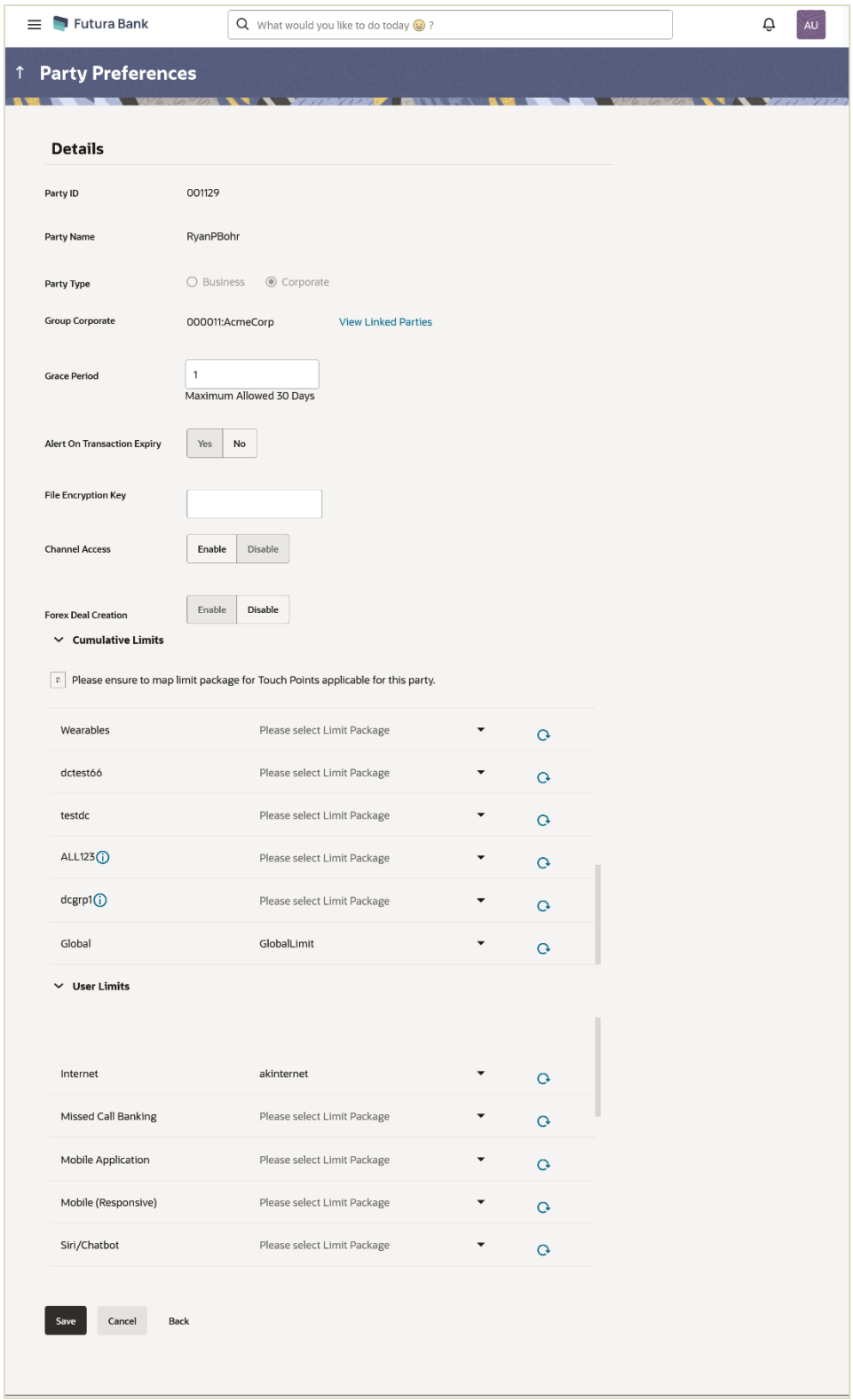
4.4 Party Preferences - Edit

Administrator can edit the party preferences maintained for a party.

To edit the customer preferences:

1. In the **Party Id** field, enter the party ID whose party preferences you want to view.
   OR
   In the **Party Name** field, enter the name of the party whose party preferences you want to view.
2. Click **Search**.
   The party preference maintained for the party ID appears based on the entered search parameters.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
3. Click **Edit** to edit the party preferences.
   The **Details** screen appears along with the party ID.

Party Preferences Maintenance – Modify



Field Description

Field Name	Description
Details	
Party ID	Party ID for which the party preference to be maintained. This field is not editable. **Note:** For Non Customer Corporates (counterparties on boarded by Corporates) the system will look for the party ID in OBSCF/OBCMS.
Party Name	Party Name of a party for which the party preference to be maintained. This field is not editable.
Party Type	Party type for which the party preference is to be maintained. This field is not editable.
Group Corporate	Group Corporate ID and Name with which the Corporate Party is to be mapped. This field is not editable. Note: This field is enabled for the **Corporate** party.
View Linked Parties	If an existing Group Corporate is selected, a link is available to view the linked parties. Click on the link to view the linked parties under a Group Corporate. Note: This field is enabled for the **Corporate** party.
Grace Period	Provision of time period is made to allow user to approve the transaction after the actual due date. **Note:** The tooltip with information will appear on dashboard in the **Pending for Approvals** section only when the user hovers on grace period.
Grace Period Expiry Alert	Enter the number of days prior to Grace Period Expiry, before which the alert needs to be sent to Maker and Approver regarding transaction approval expiry period. For e.g. if the value is set as 1 in this field then the alert should be sent one day before the grace period expiry date.

Field Name	Description
	Note: 1) The value entered in this field should be less than the value entered in **Grace Period** field. 2) If there is no **Grace Period** present, then this will not get enabled.
Occurrence	Specify the alert preference. The options are: • Recurring- an alert will be sent daily, starting from the number of days configured in the above field before the before the grace period expiry date till the transaction is approved or expired (whichever is earlier) . • One Time- an alert would be sent only once with respect to value set in Grace Period For e.g. if the grace period is set as 5 days, and the days before the alert is required to be sent is set as 3 days and the alert preference is set as recurring then an alert will be sent for 3 days in a row (daily) before the grace period expiry date or until the transaction is approved (whichever is earlier) . if this parameter is set as 'one time' then the alert would be sent only once i.e. 3 days before the grace period expiry date. **Note:** 1) The field will become 'Mandatory' if the user inputs value in the **Grace Period** Expiry **Alert** field. 2) If there is no Grace Period present, then this will not get enabled.
Alert on Transaction Expiry	Specify if the alert is required to be sent on the Transaction Expiry Date. The options are: • Yes • No **Note:** 1) The field will become 'Mandatory' if the user inputs value in the Grace Period days field. 2) If there is no Grace Period present, then this will not get enabled.
File Encryption Key	File Encryption key is the unique key provided to the corporate for encrypting/decrypting the bulk files that he is uploading.
Approval Flow	The approval type for the party.

Field Name	Description
	The options are: • Sequential • Parallel • No Approval
Channel Access	Whether users associated with a party can start transacting through the channel. The options are: • Enable : Allows bank administrator to enable the party for channel access • Disable: Allows bank administrator to disable the party for channel access
Forex Deal Creation	Whether users associated with a party can create forex deals. The options are: • Enable: If this option is enabled, corporate user associated with this party can create forex deals. • Disable: If this option is disabled, corporate user associated with this party cannot create forex deals.
Roles	Application roles mapped to the user. In case of multi entity setup, these roles will be for the default/home entity of the user. These roles are applicable only for a Business Party Type.

Cumulative Limit

It allows Bank Administrator to map customer cumulative daily limits to the party. All the touch points and touch point groups maintained the system are listed on the screen. Administrator needs to ensure that the relevant packages are mapped to all the touch points/groups accessible by the party users. Also an option is provided to map the limit package at Global level (a group created with all internal and external touch points)

All the touch points and touch point groups maintained in the system are listed under each entity. Packages can be mapped for each touch point and for a group. For Business Party transactions, the limit package maintained at the party level (as a part of party preference) shall be considered and utilized.

Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for which the limit packages are to be mapped.
Package	List of the packages available for mapping to touch points/ group are listed here. Limit packages maintained for the selected touch point will get here.

Field Name	Description
User Limits	
This field allows the Bank Administrator to map customer user level limits (CUL) to the party. All the touch points and touch point groups maintained the system are listed on the screen. Administrator needs to ensure that the relevant packages are mapped to all the touch points/groups accessible by the selected party users. Also an option is provided to map the limit package at Global level (a group created with all internal and external touch points). These limits are applicable only for a **Corporate** Party Type.	
Touch Points/ Group	Name of touch points/group maintained under a specific entity for which the user limit packages are to be mapped.
Package	List of the packages available for mapping to touch points/ group are listed

4. Update the required details.
5. Click **Save** to save Party Preference. User is directed to the **Party Preference - Review** page post necessary validations.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction and navigate back to **Dashboard**.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to make the changes if any.
   OR
   Click **Cancel** to cancel the transaction and navigate back to **Dashboard**.
7. The success message of updation appears.
   Click **OK** to complete the transaction.

FAQ

1. What is sequential type of approval flow?

Under Sequential approval flow, the approval can be done only in the sequence as mentioned in approval workflow. So, at the 1st level of approval, users/user groups who are assigned to authorize only can view and approve the transaction. After the transaction is approved by level 1 user, users/user groups having rights for 2nd level of approval will be able to view and authorize the transaction. The transaction is marked as approved only after the user at the last level approves/authorizes it.

2. What is Parallel type of approval flow?

It is “Non-Sequential” type of approval flow which doesn’t follow any specific sequence. Any user (who is part of the approval flow) from any approval level can pick up the transaction/maintenance and approve it. The transaction/maintenance is marked as approved if one user from each approval level (as configured) has approved/authorized the transaction.

3. **What is cumulative daily limit package?**

   This limit package acts as a cumulative limit for all users of a party and is utilized as and when any user authorizes the transaction as a final approver. The daily limit per transaction and number of transactions allowed limit is checked and updated against the cumulative limit set.

4. **What is User limit package?**

   This limit package is applicable for all users of the party (Users to whom this party ID is mapped as primary Party ID). This package will be overridden by User level limits package, if defined, at User level in User Management screen.

5. **Can administrator delete Party Preference?**

   No, party preference cannot be deleted but can be disabled.

6. **If I change the approval type from sequential to parallel or vice versa, what happens to the in-flight transactions/maintenances?**

   Edited approval type is applicable for new transactions initiated post modification. Previously initiated transactions (in flight transactions/maintenances) which are pending approval will follow an approval type which was applied at the time of transaction initiation.

7. **If I edit the ‘Allowed Roles field’ and remove one of the options supported earlier, what impact will it have to the existing users on-boarded on that role?**

   If the Bank administrator edits and removes the roles mapped as ‘Allowed Roles’., the removed role will not be available to corporate administrator while creating new user and editing existing user. Old users whom the role is already mapped will continue to get the privileges.

8. **Can I edit the limit packages? How does it impact the transactions?**

   Yes, new limit package can be mapped for party. Limits get applied from an immediate effect if the effective date is less than or equal to current date. And if the effective date is future date, the limit package will be applied from the date available in the package.

9. **Is it mandatory to map packages for all the touch points and groups available under each entity?**

   Mapping the limit package (CCL) for global is mandatory. However the mapping limit packages (CCL) for each touch point and for all groups is not mandatory. Whereas, administrator needs to operationally ensure that packages are mapped to the relevant touch point/groups which are accessible by the party users.

   In case of customer user limit packages (CUL), if the package will be overridden by User level limits package, if defined, at User Maintenance. Or packages maintained for a user segment at system rules will be applicable if not package mapping is not defined at user or party level.

10. **Can I manually define Global touch point group?**

No, Touch Point – Global is nothing but a group of all internal and external touch points available in the application. This group cannot be maintained manually.

5. Merchant Management

Merchant Onboarding facilitates the system administrator to set up and maintain merchants using the channel banking platform. This, in turn, enables the users to initiate merchant based payments using the channel banking facility. This is also helpful in maintaining merchant which will act as a payment aggregator for sourcing funds from external sources to the wallet account.

Using this option, the system administrator can create and maintain merchant details in the application. Administrators can map the CASA account of the merchant, to enable the merchant payments. The system administrator can also select the required remittance type to be mapped for the merchant payments while creating a merchant.

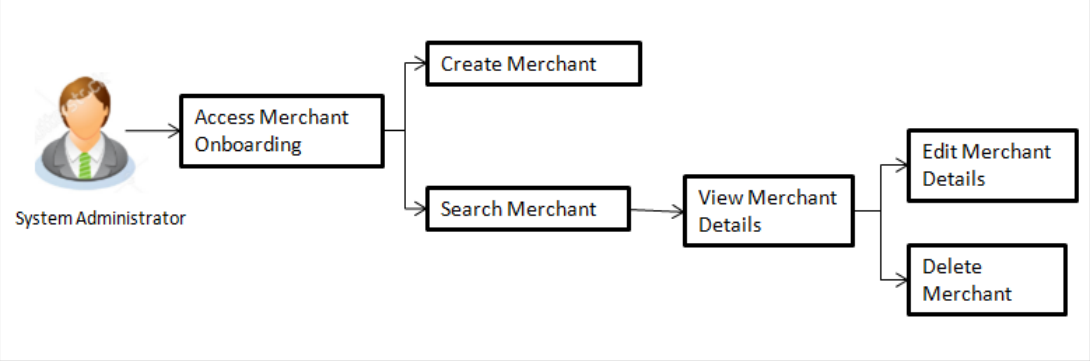
The remittance type can be:

- Funds Out
- Collect Funds

Pre-requisites

- Transaction access is provided to the System Administrator
- Approval rule set up for System Administrator to perform the actions
- Checksum type and checksum algorithm is maintained
- Enterprise roles are maintained in the application
- Merchant's account is maintained in the host system

Workflow



Features Supported In Application

The following features are available for merchant maintenance:

- Create Merchant
- View Merchant Details
- Edit Merchant details
- Delete Merchant

How to reach here:

System Administrator Dashboard > Onboarding > Merchant Onboarding > Merchant Management
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Onboarding > Merchant Management

Note: This functionality is only available for QR based merchant payment.

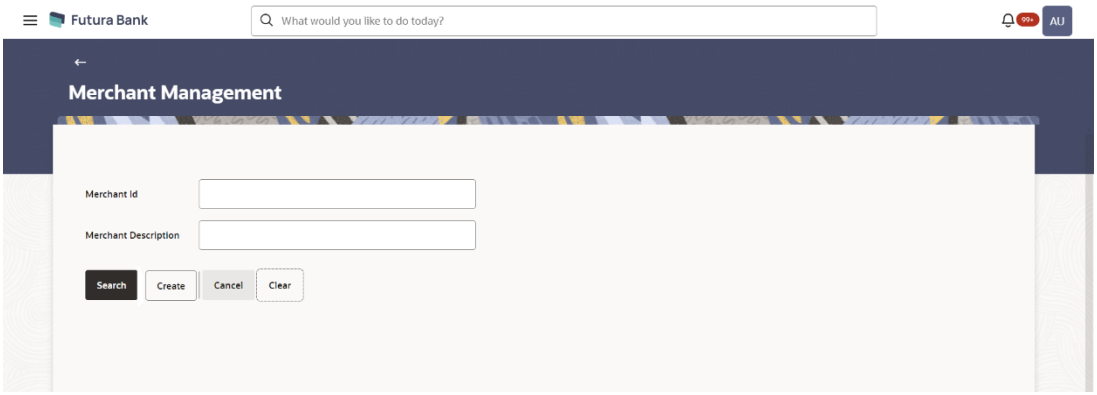
5.1 Merchant Management – Search

From this screen, the administrator is able to search existing merchant maintenances based on the search parameters provided. On being displayed the search results based on the search criteria defined, the administrator is able to view the details of any merchant maintenance by selecting a record.

To search merchant:

1. Navigate to the **Merchant Management** screen.

Search Merchant



Field Description

Field Name	Description
Merchant Id	Enter the unique ID of the merchant whose details you want to view.
Merchant Description	Enter the description of the merchant whose details you want to view.

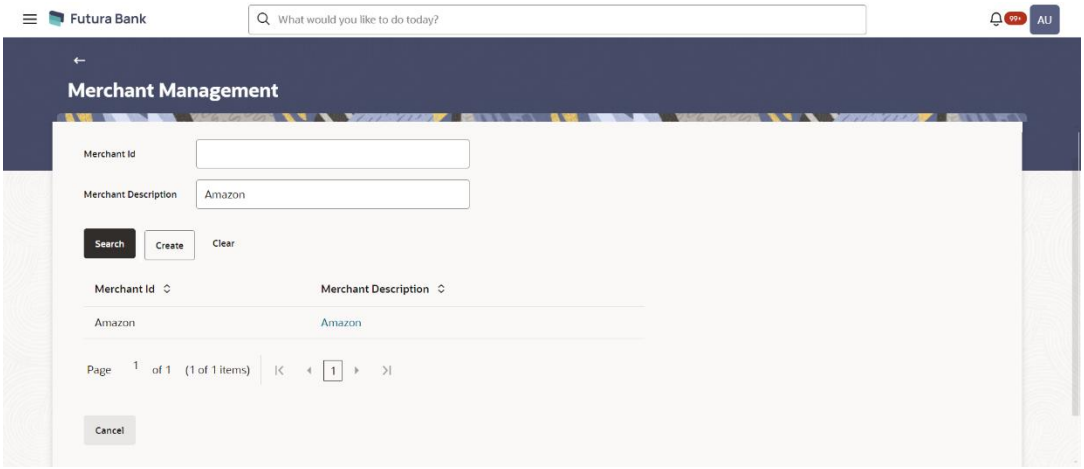
2. In the **Merchant Id** field, enter the unique id of the merchant.
   OR
   In the **Merchant Description** field, enter the description of the merchant.

3. Click **Search**. The **Merchant Management** screen with search results appears based on the search parameters.
   OR
   Click **Clear,** if you want to reset the search parameters.
   OR
   Click **Cancel,** if you want to cancel the transaction.

   OR

   Click **Create** to create another merchant maintenance.

Merchant Management - Search Results



Field Description

Field Name	Description
Merchant Id	The facility to search for a specific merchant maintenance record on the basis of the unique ID/key assigned to the merchant by the bank.
Merchant Description	The facility to search for a specific merchant maintenance based on the description of the merchant.

Search Results

The following details are displayed per merchant record which are retrieved based on the search criteria identified in the fields defined above.

Merchant Id	The unique ID/key assigned to the specific merchant by the bank.
Merchant Description	The description of the merchant corresponding to the merchant Id.

4. To view the details of a specific merchant, click the record. The **Merchant Management - View** screen appears.

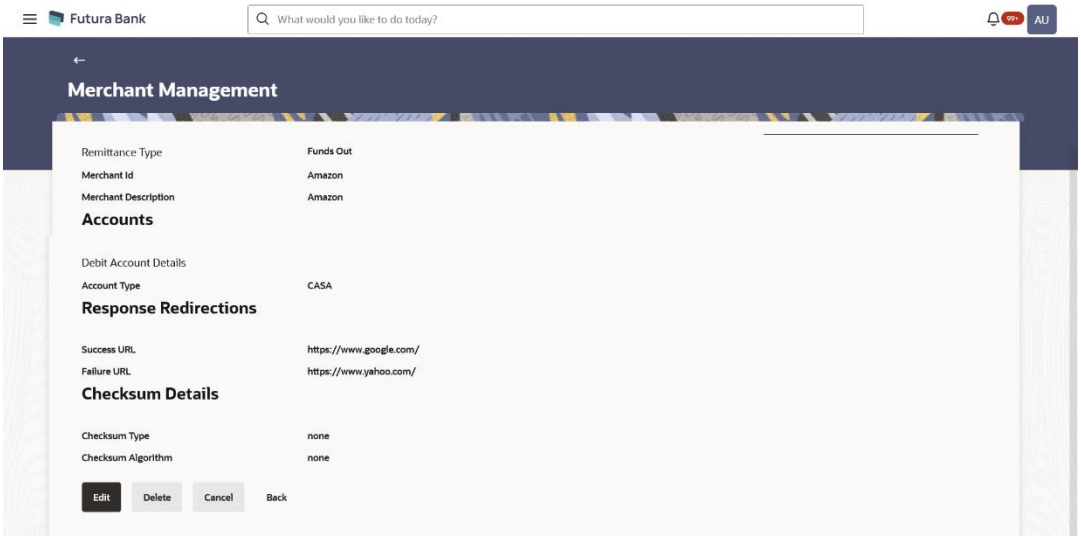
5.2 Merchant Management – Funds Out

The Merchant Management screen allows the system administrator to view, create, edit and delete the merchant details.

5.2.1 Merchant Management – Funds Out – View

On selecting a specific merchant record by clicking on the link provided on the merchant description, the screen displaying the details of the selected merchant.

Merchant Management – Funds Out- View



Field Description

Field Name	Description
Remittance Type	The type or remittance mapped to the merchant. The remittance type can be: • Funds Out • Collect Funds
Merchant Id	The unique ID/key assigned to the merchant by the bank.
Merchant Description	The description of the merchant.
Accounts	
Debit Account Details	

Field Name	Description
Account Type	Displays the type of account i.e. GL or CASA account, associated with the merchant.
Account Number	Displays the merchant's debit account number.
Response Redirections	
Success URL	The URL for sending the response of the transaction if it is a successful transaction.
Failure URL	The URL for sending the dynamic response of the transaction if it is a failed transaction.
Checksum Details	
Checksum Type	The checksum type.
Checksum Algorithm	The checksum algorithm.
Security Key	Input the security key. This field appears if a value is selected in **Checksum Algorithm** drop-down list.

1. Click **Edit** to edit merchant details. The user is directed to the **Merchant Management - Edit** screen.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.

   OR

   Click **Delete** to delete the merchant maintenance.

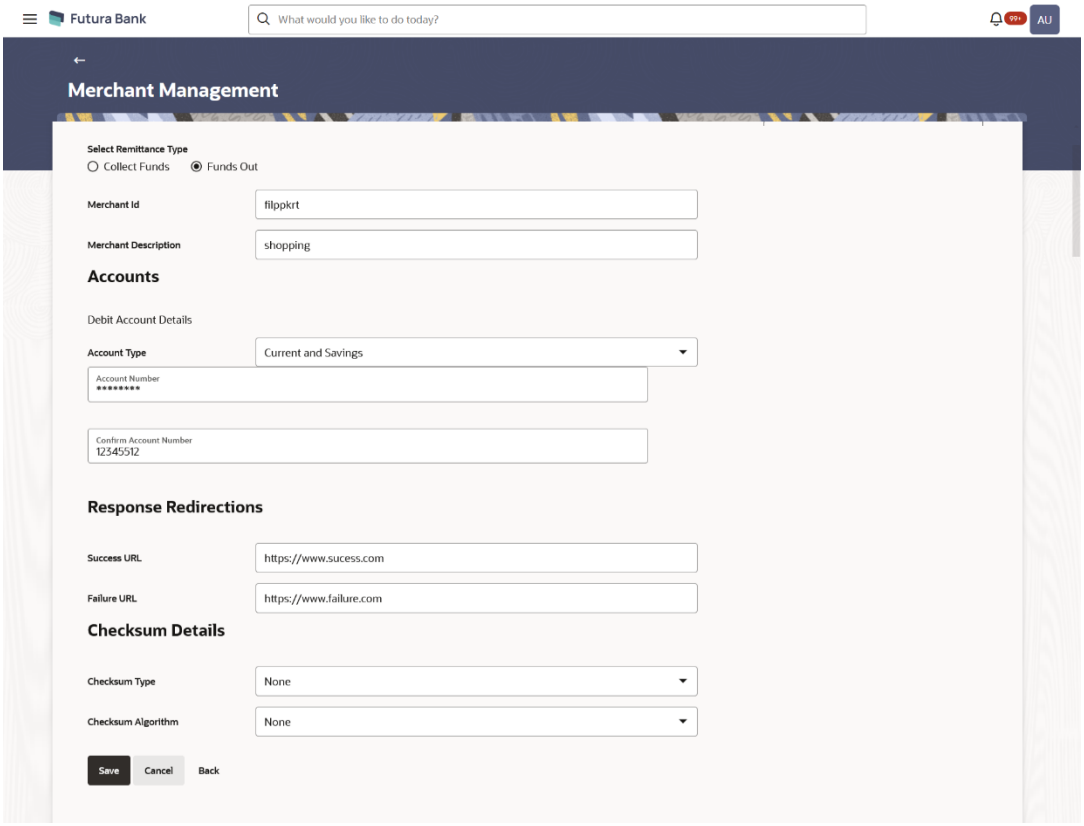
5.2.2 Merchant Management – Funds Out – Create Merchant

The system administrator can create a new merchant so that the bank's customers can make payments to the merchant using channel banking or by scanning the QR code of the Merchant without entering merchant account details.

To create a merchant:

1. In the **Merchant Maintenance screen, c**lick **Create**. The **Merchant Management – Create** screen appears.

Merchant Management - Funds Out- Create



Field Description

Field Name	Description
Select Remittance Type	The type or remittance to be mapped to the merchant. The remittance type can be: • Funds Out • Collect Funds

Field Name	Description
Merchant Id	Specify a unique ID by which the merchant will be identified.
Merchant Description	Enter a description of the merchant.
Accounts	
Debit Account Details	
Account Type	Specify the type of account i.e. GL or CASA account, associated with the merchant.
Account Number	Specify the merchant's debit account number.
Confirm Account Number	Re-enter the merchant's account number to confirm the same if the account number has been changed.
Response Redirections	
Success URL	Specify the URL for sending the response of the transaction if it is a successful transaction.
Failure URL	Specify the URL for sending the response of the transaction if it is a failed transaction.
Checksum Details	
Checksum Type	Specify the checksum type.
Checksum Algorithm	Specify the checksum algorithm.
Security Key	Input the security key. This field appears if a value is selected in **Checksum Algorithm** drop-down list.

2. In the **Merchant Id** field, enter the ID of the merchant.
3. In the **Merchant Description** field, enter the description of the merchant.
4. Under the section **Debit Account Details**, from the **Account Type** list, select the appropriate account type.
5. In the **Account Number** field, enter the account number of the merchant corresponding to the account type selected.
6. In the **Confirm Account Number** field, re-enter the merchant's account number.

7. Under the **Response Redirections** section,
   a. In the **Success URL** field, enter the valid URL.
   b. in the **Failure URL** field, enter the valid URL.
8. Under the **Checksum Details** section,
   a. From the **Checksum Type** drop-down list, select the checksum type.
   b. From the **Checksum Algorithm** drop-down list, select the checksum algorithm.
      i. In the **Security Key** field, enter the security key.
9. Click **Save** to save the Merchant details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
10. The **Review** screen appears, verify the details and click **Confirm** to confirm the details.
    OR
    Click **Edit** to make changes if any.
    The administrator is directed to **Merchant Management – Create** screen with values in editable form.
    OR
    Click **Cancel** to cancel the operation and to navigate back to 'Dashboard'.
11. The success message appears along with the status of the transaction. Click **OK**.

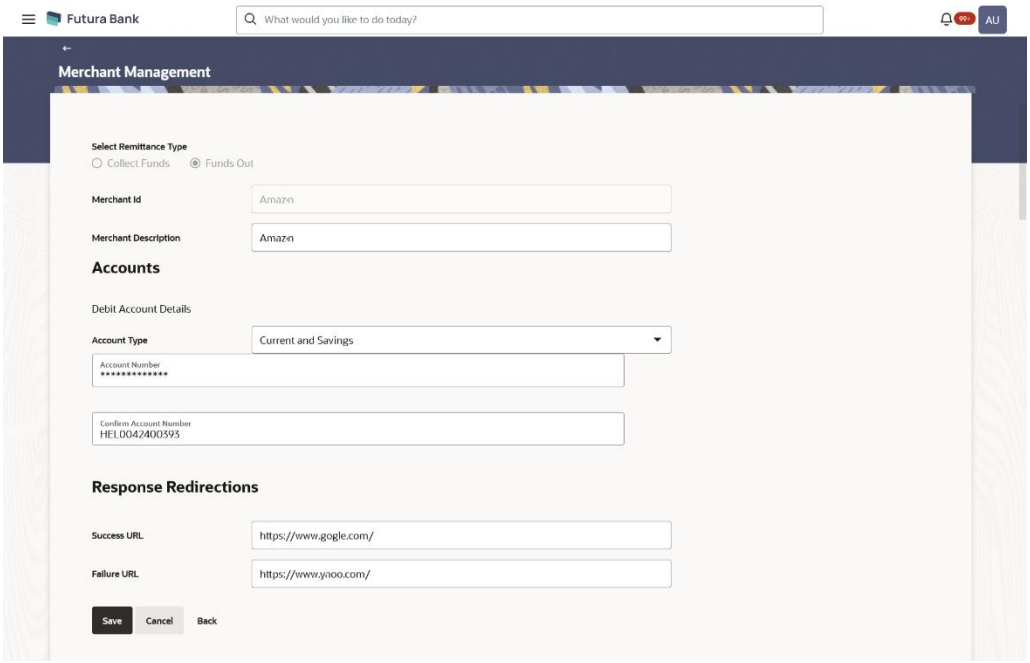
5.2.3 Merchant Management – Funds Out – Edit

The system administrator can edit the details of any merchant maintained in the application. In order to edit the details of any merchant, the user must select the **Edit** option provided on Merchant Management – View (details) page of the specific merchant.

To edit a merchant:

1. Navigate to the **Merchant Management** screen and in the **Merchant Id** field, enter the unique id of the merchant whose details you want to edit.
   OR
   In the **Merchant Description** field, enter the description of the merchant whose details you want to edit.
2. Click **Search**. The search results appear based on the search parameters defined.
3. Select the merchant record of which details you want to edit, by selecting the link provided on the merchant description. The **Merchant Management** – **View** screen appears.
4. Click the **Edit** option available on the Merchant **Management**– View screen to edit merchant details. The administrator is directed to the **Merchant Management - Edit** screen.

Merchant Management – Funds Out - Edit



Field Description

Field Name	Description
Select Remittance Type	The type or remittance mapped to the merchant. The remittance type can be: • Funds Out • Collect Funds
Merchant Id	The unique ID assigned to the merchant by the bank. This field cannot be edited.
Merchant Description	The description of the merchant. This field is editable.
Accounts	
Debit Account Details	
Account Type	The type of account associated with the merchant, e.g. CASA. This field is editable.
Account Number	The merchant's debit account number. This field is editable.

Field Name	Description
Confirm Account Number	Re-enter the merchant's account number to confirm the same if the account number has been changed. This field is editable.
Response Redirections	
Success URL	The URL for sending the response of the transaction if it is a successful transaction.
Failure URL	The URL for sending the response of the transaction if it is a failed transaction.
Checksum Details	
Checksum Type	The checksum type. This field is editable.
Checksum Algorithm	The checksum algorithm. This field is editable.
Security Key	Input the security key. This field is editable. This field appears only if a value is selected in **Checksum Algorithm** drop-down list.

5. Update the required fields, click **Save to save the changes**.
   OR
   Click **Cancel** to cancel edit of the merchant maintenance.
   OR
   Click **Back** to navigate to the previous screen.
6. The **Review** screen appears, verify the details and click **Confirm** to confirm the details.
   OR
   Click **Edit** to make the changes if any.
   The administrator is directed to **Merchant Management – Edit** screen with all values (other than Merchant ID) in editable form.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
7. The success message appears along with the status of the transaction.
8. Click **OK**.

5.3 Merchant Management – Collect Funds

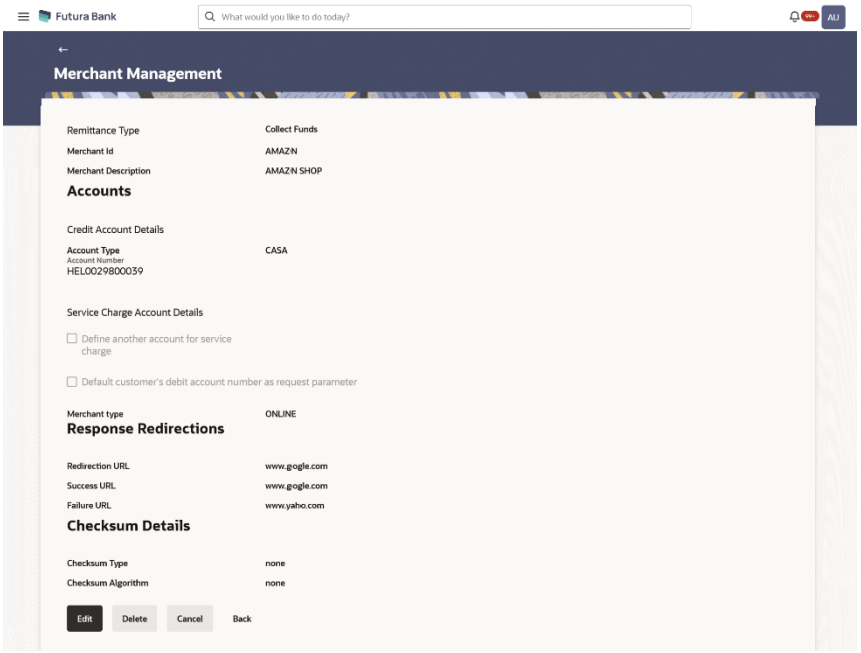
Collect Funds refers to money being received to merchant's account/s through Electronic Payment interface (EPI). The Merchant Management screen allows the system administrator to view, create, edit and delete the inward merchant details.

Using this maintenance System/Bank administrator can save the details of Payment aggregator which will act as a medium for transferring the funds to user's wallet account from the external source (Credit card/ Debit card/ Net banking).

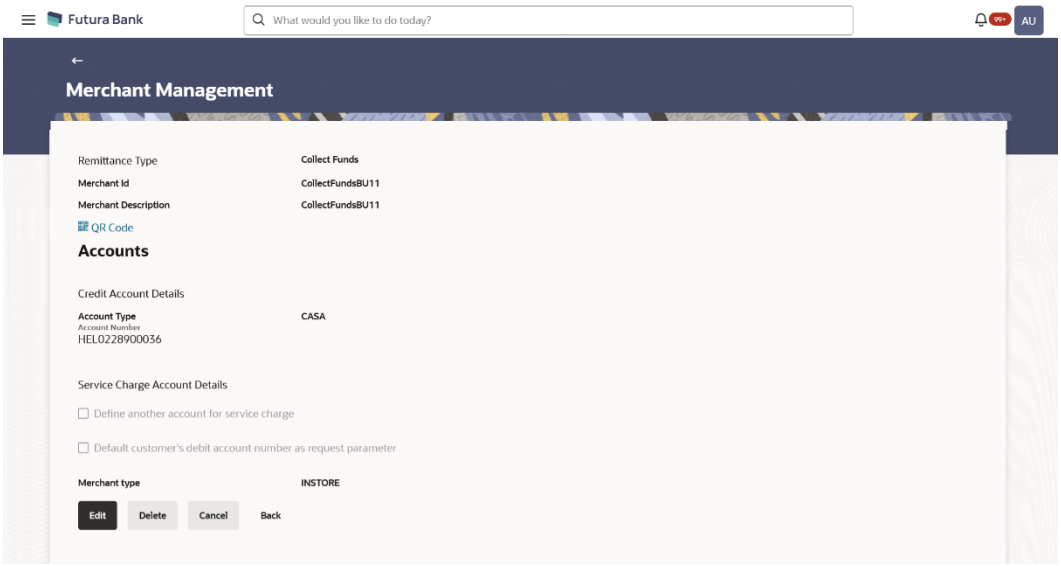
5.3.1 Merchant Management – Collect Funds – View

On selecting a specific merchant record by clicking on the link provided on the merchant description, the screen displaying the details of the selected inward remittance merchant is displayed.

Merchant Management – Collect Funds (ONLINE) – View



Merchant Management – Collect Funds (In Store) – View



Field Description

Field Name	Description
Remittance Type	The type or remittance mapped to the merchant. The remittance type can be: • Funds Out • Collect Funds
Merchant Id	The unique ID/key assigned to the merchant by the bank.
Merchant Description	The description of the merchant.
QR Code	Click the QR code link to view the QR code assigned to the merchant.
Accounts	
Credit Account Details	
Account Type	The type of account associated with the merchant, Only CASA type of accounts are supported.
Account Number	The merchant's account number.

Field Name	Description
Service Charge Account Details	
Define another account for service charge	This checkbox is selected if the merchant has another account defined for service charge.
Account Type	The service charge account type associated with the merchant e.g. CASA account. This field appears if **Define Account number for service charge** check box is selected.
Account Number	The merchant's account number. This field appears if **Define Account number for service charge** check box is selected.
Default customer's debit account number as request parameter	This check box is selected if the customer's debit account number is defaulted as request parameter.
Merchant Type	Displays the merchant type. It could be: • Online • In store
Response Redirections	
This section is displayed only for the **Online** type of merchant.	
Redirection URL	The URL for sending the response of the transaction for redirection.
Success URL	The URL for sending the response of the transaction if it is a successful transaction.
Failure URL	The URL for sending the response of the transaction if it is a failed transaction.
Checksum Details	
This section is displayed only for the **Online** type of merchant.	
Checksum Type	The checksum type.
Checksum Algorithm	The checksum algorithm.

Field Name	Description
Security Key	Enter the security key. This field appears if a value is selected in **Checksum Algorithm** drop-down list.

1. Click **Edit** to edit merchant details. The user is directed to the **Merchant Management - Edit** screen.
   OR
   Click **Back** to navigate to the previous screen**.**
   OR
   Click **Cancel** to cancel the transaction.

   OR

   Click **Delete** to delete the merchant maintenance.

QR code

The QR code is displayed if the system administrator clicks on the QR code link on the Merchant Management details screen. The administrator is provided with the facility to download the QR code so as to send it to the merchant through any offline mode.

2. Click to download the QR Code image of the merchant.

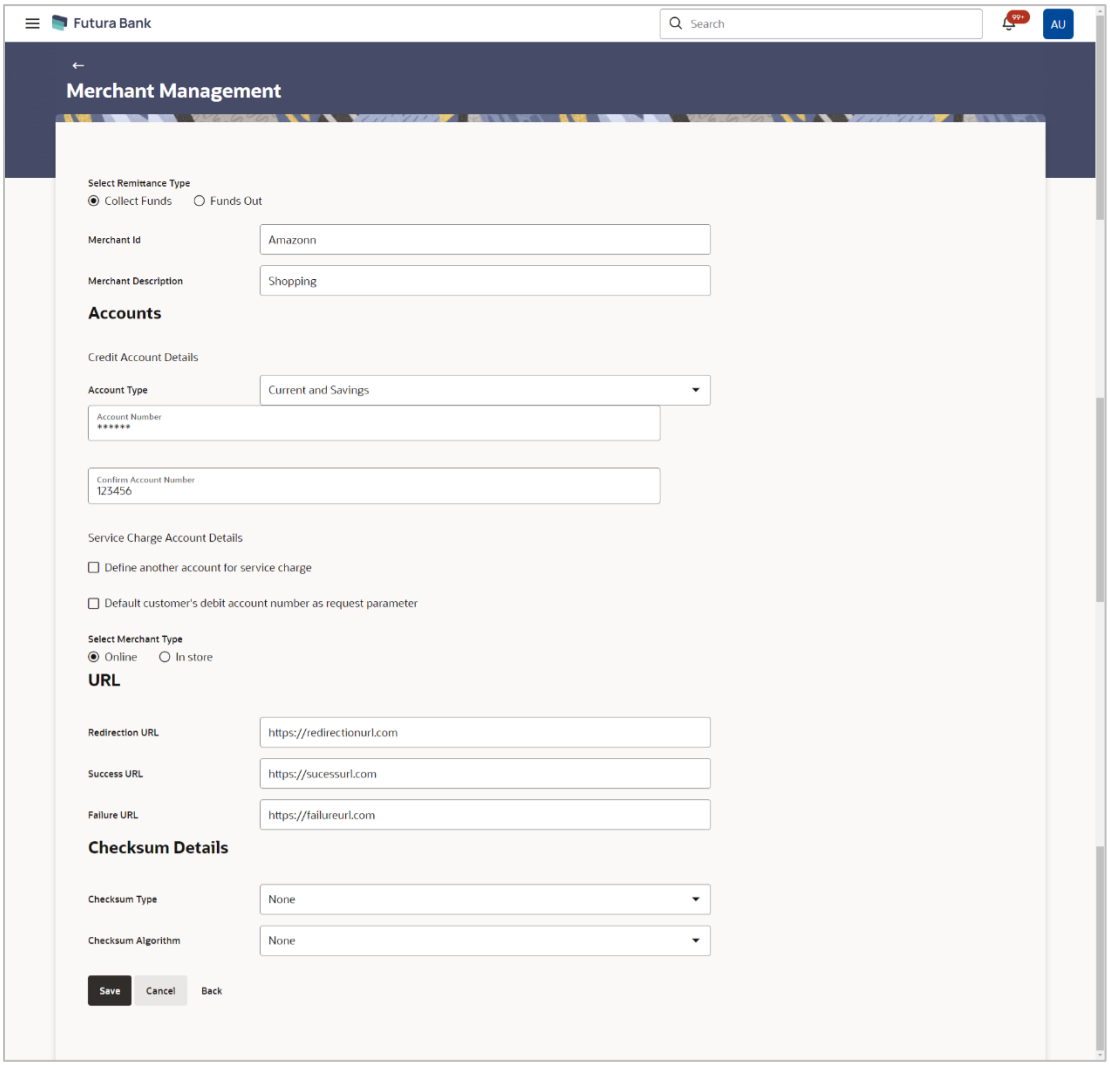
5.3.2 Merchant Management – Collect Funds – Create Merchant

The system administrator can create a new collect funds remittance merchant so that the bank's customers can receive payments in their wallet using the merchant (payment aggregator) using channel banking.

To create a merchant:

1. In the **Merchant Maintenance screen, c**lick **Create**. The **Merchant Management – Create** screen appears.

Merchant Management – Collect Funds - Create



Field Description

Field Name	Description
Select Remittance Type	The type or remittance to be mapped to the merchant. The remittance type can be: • Funds Out • Collect Funds
Merchant Id	Specify a unique ID by which the merchant will be identified.
Merchant Description	Enter a description of the merchant.
Accounts	
Credit Account Details	
Account Type	Specify the type of account associated with the merchant, Only CASA type of accounts are supported.
Account Number	Specify the merchant's credit account number.
Confirm Account Number	Re-enter the merchant's account number to confirm the same if the account number has been changed.
Service Charge Account Details	
Define another account for service charge	This checkbox is selected if the merchant has another account defined for service charge.
Account Type	The service charge account type associated with the merchant e.g. CASA account. This field appears if **Define Account number for service charge** check box is selected.
Account Number	The merchant's account number. This field appears if **Define Account number for service charge** check box is selected.
Confirm Account Number	Re-enter the merchant's account number to confirm the same if the account number has been changed.
Default customer's debit account number as request parameter	This check box is selected if the customer's debit account number is defaulted as request parameter.

Field Name	Description
Select Merchant Type	Specify the merchant type. The options are: • Online • In store

Generated QR code can be downloaded from view merchant, if the **Merchant Type** is selected as **In Store**.

URL

This section is displayed only for the **Online** type of merchant.

Redirection URL	Specify the URL for sending the response of the transaction for redirection.
Success URL	Specify the URL for sending the response of the transaction if it is a successful transaction.
Failure URL	Specify the URL for sending the response of the transaction if it is a failed transaction.

Checksum Details

This section is displayed only for the **Online** type of merchant.

Checksum Type	Specify the checksum type.
Checksum Algorithm	Specify the checksum algorithm.
Security Key	Enter the security key. This field appears if a value is selected in **Checksum Algorithm** drop-down list.

2. In the **Merchant Id** field, enter the ID of the merchant.
3. In the **Merchant Description** field, enter the description of the merchant.
4. Under the section **Credit Account Details,** from the **Account Type** list, select the appropriate account type.
5. In the **Account Number** field, enter the account number of the merchant corresponding to the account type selected.
6. In the **Confirm Account Number** field, re-enter the merchant's account number.
7. Under the **Response Redirections** section,
    a. In the **Success URL** field, enter the valid URL.
    b. in the **Failure URL** field, enter the valid URL.
8. Under the **Checksum Details** section,
    a. From the **Checksum Type** drop-down list, select the checksum type.
    b. from the **Checksum Algorithm** drop-down list, select the checksum algorithm.
        i. In the **Security Key** field, enter the security key.
9. Under the **Service Charge Details** section,
10. Select the checkbox next to **Define another account for service charge** if the merchant has a different account specified for service charges.
    a. From the **Account Type** list, select the appropriate account type.
    b. In the **Account Number** field, enter the account number of the merchant corresponding to the account type selected.
    c. In the **Confirm Account Number** field, re-enter the merchant's account number.
11. Select the checkbox against the **Default customer's debit account number as request parameter** if the customer's debit account number is defaulted as request parameter.
12. If the **Merchant Type** is selected as **Online** in the **Select Merchant Type** field, enter the details below in the **URL** section.
    a. In the **Redirection URL** field, enter the valid URL.
    b. In the **Success URL** field, enter the valid URL.
    c. In the **Failure URL** field, enter the valid URL.
13. If the **Merchant Type** is selected as **Online** in the **Select Merchant Type** field, enter the details below in the **Checksum Details** section.
    a. From the **Checksum Type** drop-down list, select the checksum type.
    b. From the **Checksum Algorithm** drop-down list, select the checksum algorithm.
        i. In the **Security Key** field, enter the security key.
14. Click **Save** to save the Merchant details.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.

15. The **Review** screen appears, verify the details and click **Confirm** to confirm the details.
    OR
    Click **Edit** to make changes if any.
    The administrator is directed to **Merchant Management – Create** screen with values in editable form.
    OR
    Click **Cancel** to cancel the operation and to navigate back to 'Dashboard'.
16. The success message appears along with the status of the transaction. Click **OK**.

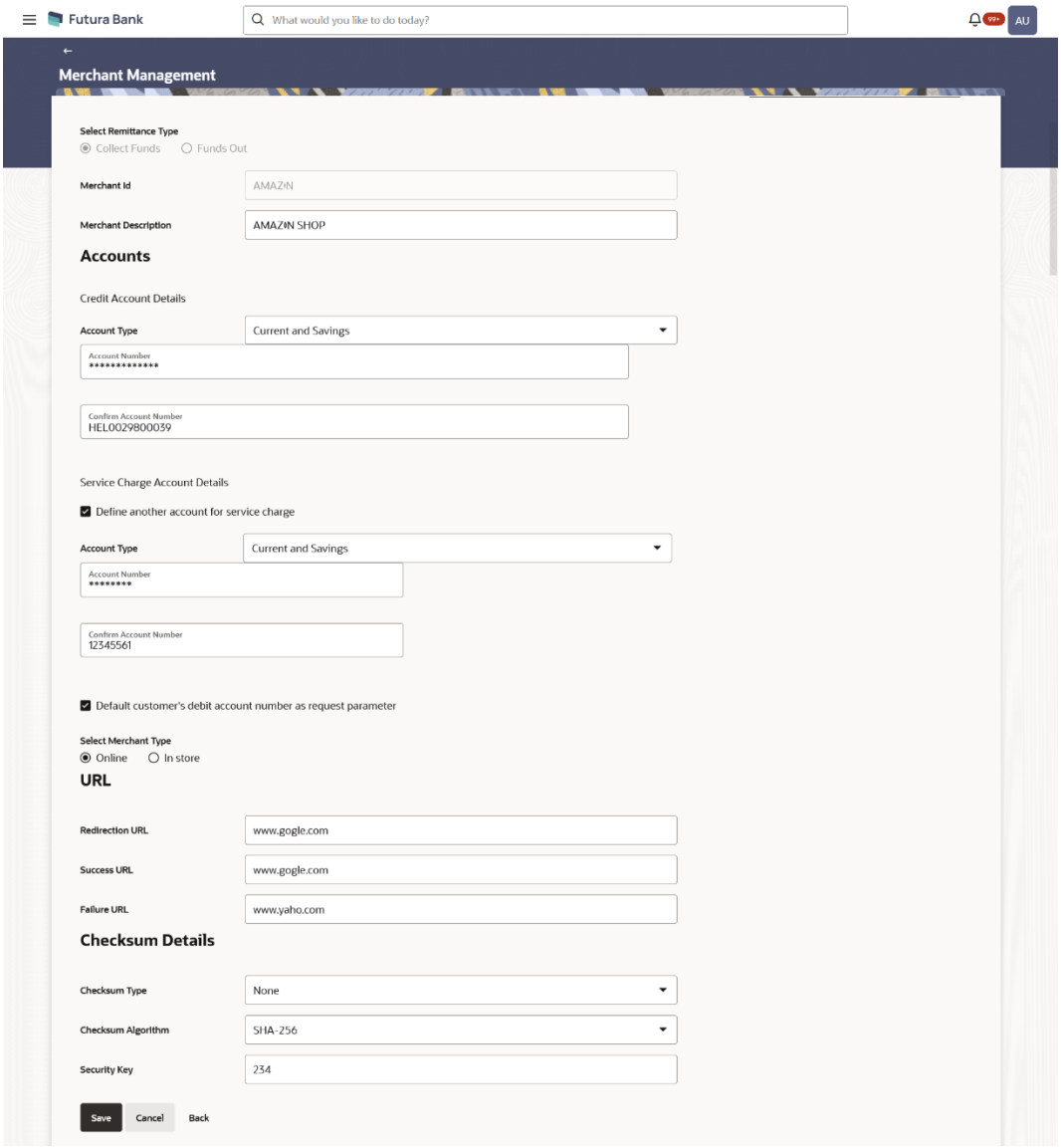
5.3.3 Merchant Management – Collect Funds – Edit

The system administrator can edit the details of any collect funds remittance merchant maintained in the application. In order to edit the details of any merchant, the user must select the **Edit** option provided on Merchant Management – View (details) page of the specific merchant.

To edit a merchant:

1. Navigate to the **Merchant Management** screen and in the **Merchant Id** field, enter the unique id of the merchant whose details you want to edit.
   OR
   In the **Merchant Description** field, enter the description of the merchant whose details you want to edit.
2. Click **Search**. The search results appear based on the search parameters defined.
3. Select the merchant record of which details you want to edit, by selecting the link provided on the merchant description. The **Merchant Management** – **View** screen appears.
4. Click the **Edit** option available on the Merchant **Management**– **View** screen to edit merchant details. The administrator is directed to the **Merchant Management - Edit** screen.

Merchant Management – Collect Funds - Edit



Field Description

Field Name	Description
Select Remittance Type	The type or remittance mapped to the merchant. The remittance type can be: • Funds Out • Collect Funds

Field Name	Description
Merchant Id	The unique ID assigned to the merchant by the bank. This field cannot be edited.
Merchant Description	The description of the merchant. This field is editable.
Accounts	
Credit Account Details	
Account Type	The type of account associated with the merchant, Only CASA type of accounts are supported. This field is editable.
Account Number	The merchant's credit account number. This field is editable.
Confirm Account Number	Re-enter the merchant's account number to confirm the same if the account number has been changed.
Service Charge Account Details	
Define another account for service charge	This checkbox is selected if the merchant has another account defined for service charge.
Account Type	The service charge account type associated with the merchant e.g. CASA account. This field appears if **Define Account number for service charge** check box is selected.
Account Number	The merchant's account number. This field appears if **Define Account number for service charge** check box is selected.
Confirm Account Number	Re-enter the merchant's account number to confirm the same if the account number has been changed.
Default customer's debit account number as request parameter	This check box is selected if the customer's debit account number is defaulted as request parameter.

Field Name	Description
Select Merchant Type	Specify the merchant type. The options are: • Online • In store
URL	
This section is displayed only for the **Online** type of merchant.	
Redirection URL	The URL for sending the response of the transaction for redirection.
Success URL	The URL for sending the response of the transaction if it is a successful transaction.
Failure URL	The URL for sending the response of the transaction if it is a failed transaction.
Checksum Details	
This section is displayed only for the **Online** type of merchant.	
Checksum Type	The checksum type. This field is editable.
Checksum Algorithm	The checksum algorithm. This field is editable.
Security Key	Input the security key. This field is editable. This field appears if a value is selected in **Checksum Algorithm** drop-down list.

5. Update the required fields, click **Save to save the changes**.
   OR
   Click **Cancel** to cancel edit of the merchant maintenance.
   OR
   Click **Back** to navigate to the previous screen.
6. The **Review** screen appears, verify the details and click **Confirm** to confirm the details.
   OR
   Click **Edit** to make the changes if any.
   The administrator is directed to **Merchant Management – Edit** screen with all values (other than Merchant ID) in editable form.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
7. The success message appears along with the status of the transaction. Click **OK**.

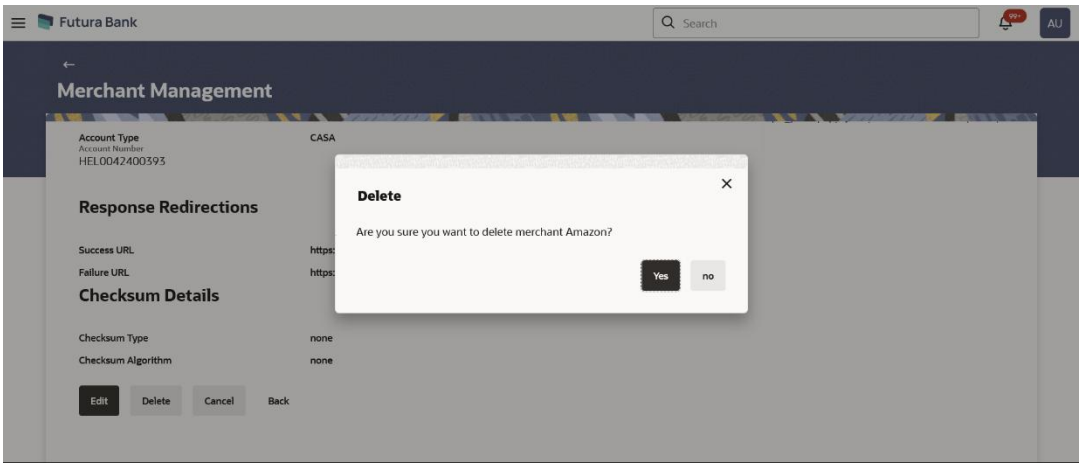
5.4 Merchant Management - Delete

The System administrator can delete any merchant maintained in the application.

To delete a merchant:

1. Navigate to the **Merchant Management** screen and in the **Merchant Id** field, enter the unique ID of the merchant whose maintenance you want to delete
   OR
   In the **Merchant Description** field, enter the description of the merchant whose maintenance you want to delete.
2. Click **Search**. The search results appear based on the search parameters defined.
3. Select the merchant record whose maintenance you want to delete, by selecting the link provided on the merchant description. The **Merchant Management** – **View** screen appears.
4. Click the **Delete** option available on the **Merchant Management – View** screen.
5. The application displays a popup message to confirm the deletion..

Merchant Management - Delete



   a. Click **Yes** to delete the merchant. A confirmation page appears with a success message and the status of deletion.
      OR
      Click **No** if you do not wish to delete the Merchant Maintenance.
6. Click **OK**.

FAQ

1. **Who can create or edit merchants?**

   The System administrator can create and edit the merchants.

2. **Can I specify the account number which is not held within this Bank?**

No, Merchant account number/GL should be of the same bank.

3. **When will the newly added merchants be available to customers?**

   Newly added merchants will be made available to the customers with immediate effect.

4. **What is the significance of defining separate account numbers for service charge account?**

   Service charges, if applicable, for an online transaction initiated by a customer will be accounted separately in the merchant's account number maintained for service charge credits.

7.

6. Limits Definition

Limits are defined by the bank to set up amount and duration based restrictions on the transactions that can be carried out by the user.

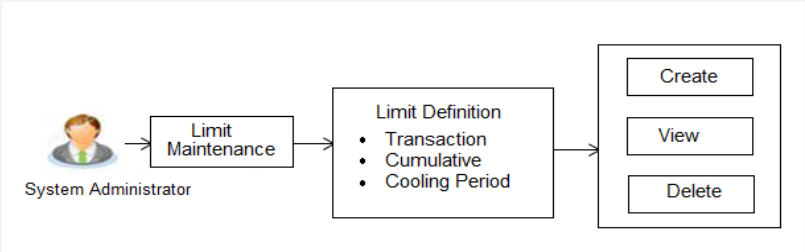
As part of limits definition maintenance, following types of limits can be defined:

- Transaction: It is the initiation limit with minimum and maximum amount defined typically for a user with role 'Maker'
- Cumulative: It is the collective transaction amount limit for all the transactions that can be performed during a day/month and maximum number of transaction in a day/month
- Cooling Period: Payee cooling period limit is a time and the amount limit set by the bank during which fund transfer is not allowed or allowed till the specified limit, to a newly added payee.
- Limit package maintenance allows the administrator to map these definitions to every transaction.

Pre-Requisites

- Transaction access is provided to System Administrator.
- Approval rule set up for System Administrator to perform the actions.

Workflow



Features supported in application

Using this option system administrator can perform the following actions:

- Search/ View Limits
- Create Limit
- Delete Limits

How to reach here:

System *Administrator Dashboard > Limits > Limits Definition*
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Limits > Limits Definition

6.1 Limits Definition - View

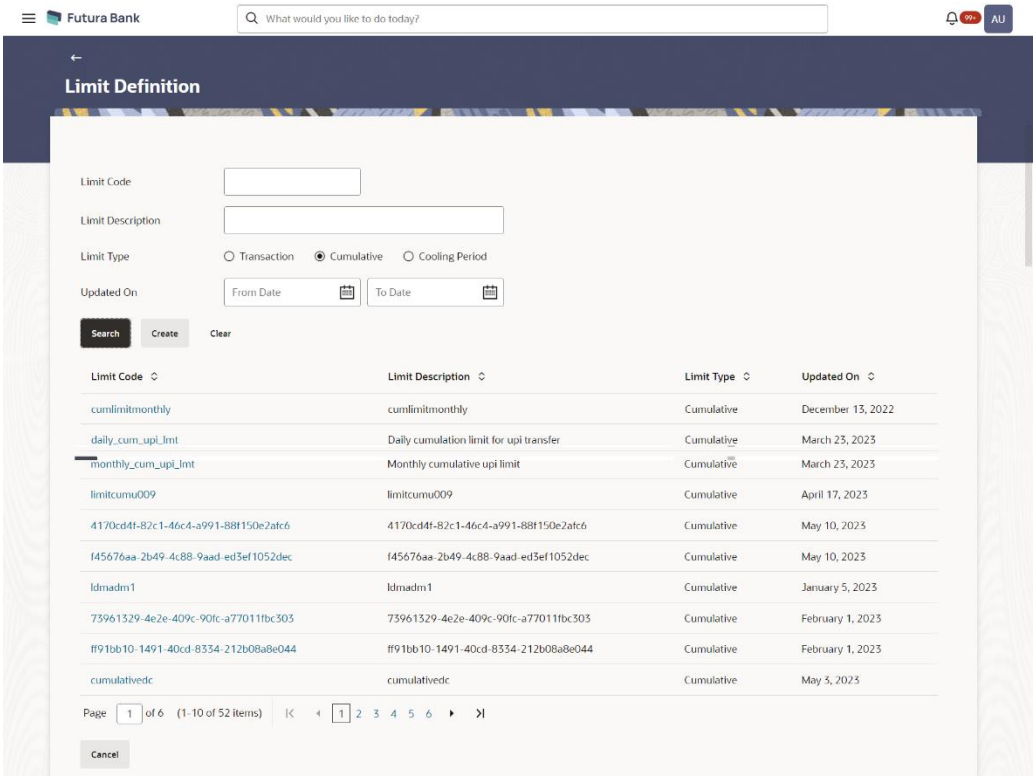
Using this option, administrator can search for particular limit based on different search parameters. The search results displays a limit list based on different search filters selected.

If the search parameters are not specified, records of all the limits maintained in the application for selected limit type are displayed.

To search and view limits:

1. In the **Limits Definition** screen, enter the search parameters and click **Search**. The **Limits Definition** screen with search results appears based on the searched criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.

Limits Definition - Search

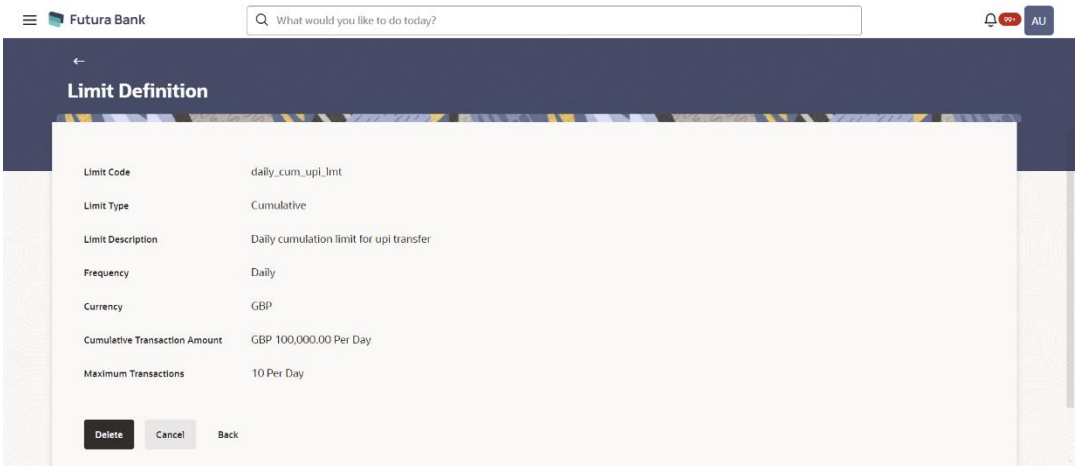


Field Description

Field Name	Description
Limit Code	Name of the limit with unique identifier.
Limit Description	Description of the limit.
Limit Type	The limit type are: • Transaction – It is the initiation limit with minimum and maximum amount • Cumulative – It is a duration based cumulative limit with maximum amount and number of transactions for a day/month • Cooling Period – Payee cooling period limit is a time and the amount limit set by the bank during which fund transfer is not allowed or allowed till the specified limit, to a newly added payee.
Search Results	
Limit Code	Name of the limit with unique identifier.
Limit Description	Description of the limit.
Limit Type	The limit type are: • Transaction – It is the initiation limit with minimum and maximum amount • Cumulative – It is a duration based cumulative limit with max amount and number of transactions for a day/month • Cooling Period – Payee cooling period limit is a time and the amount limit set by the bank during which fund transfer is not allowed or allowed till the specified limit, to a newly added payee.

2. Click the **Limit Code** of the record to view the details. The **Limits Definition -View** screen appears.

Limits Definition - View



3. Click **Delete** to delete the limit.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction and navigate back to dashboard.

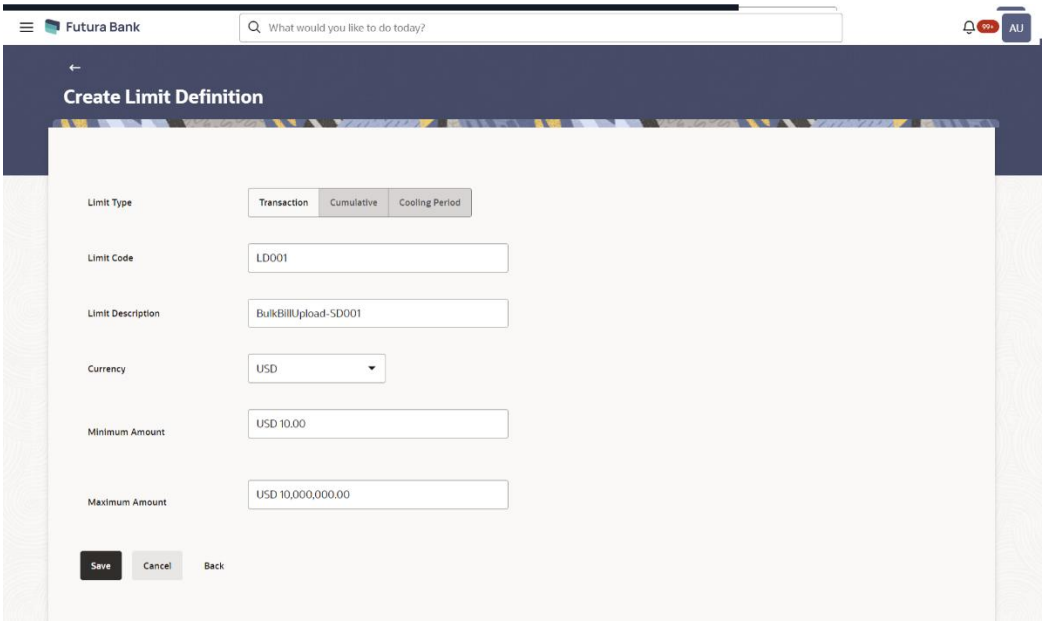
6.2 Limits Definition - Create

Using this option, System Administrator can create a limit as required.

To create a transaction limit:

1. In the **Limits Definition** screen, click **Create**. The **Limits Definition - Create** screen with **Transaction** tab appears.

Limits Definition - Transaction - Create



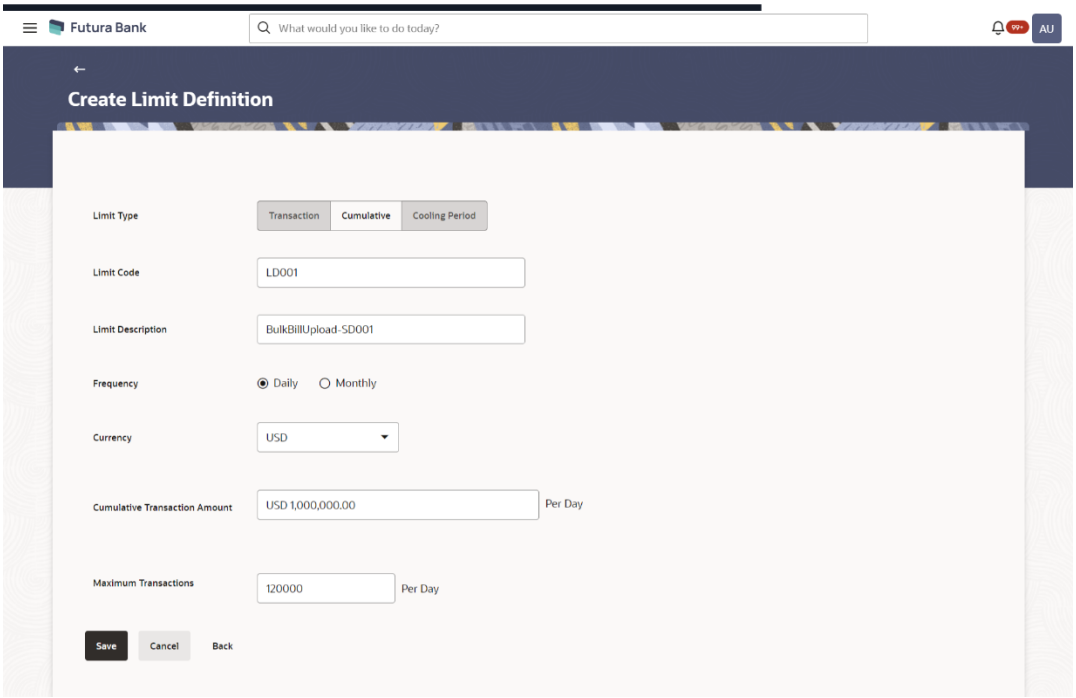
Field Description

Field Name	Description
Limit Type	The type of limit. The limit type for selection are: • Transaction – It is the initiation limit with minimum and maximum amount • Cumulative – It is a duration based limit with maximum amount and number of transactions for a day/month • Cooling Period – Payee cooling period limit is a time and the amount limit set by the bank during which fund transfer is not allowed or allowed till the specified limit, to a newly added payee.
Limit Code	The name of the limit with unique identifier.

Field Name	Description
Limit Description	Description of the limit.
Currency	The currency to be set for the limit.
Minimum Amount	The minimum amount for a transaction in selected currency.
Maximum Amount	The maximum amount for a transaction in selected currency.

2. In the **Transaction** tab screen, enter the code in the **Limit Code** field.
3. In the **Limit Description** field, enter the description of the limit.
4. From the **Currency** field, select the appropriate currency for the limits.
5. In the **Minimum Amount** and **Maximum Amount** field, enter the minimum and maximum amount for a transaction in local currency.
6. Click **Save** to save the created limit.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction and navigate back to dashboard.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
8. The success message of transaction submission appears.
   Click **OK** to complete the transaction.

Limits Definition - Cumulative - Create



Field Description

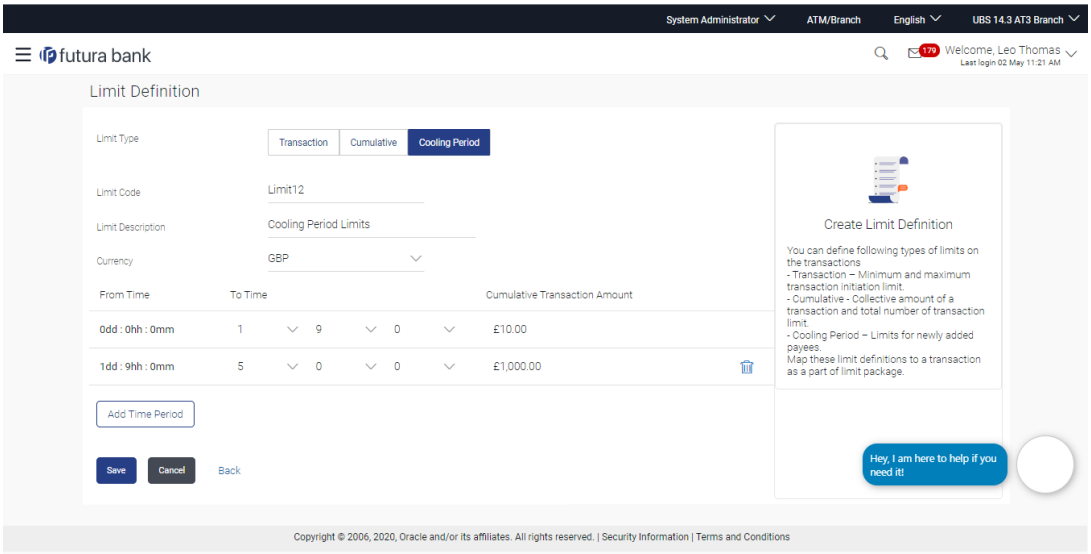
Field Name	Description
Limit Type	The type of limit. The limit type for selection are: • Transaction – It is the initiation limit with minimum and maximum amount • Cumulative – It is a duration based limit with maximum amount and number of transactions for a day/month • Cooling Period – Payee cooling period limit is a time and the amount limit set by the bank during which fund transfer is not allowed or allowed till the specified limit, to a newly added payee.
Limit Code	The name of the limit with unique identifier.
Limit Description	Description of the limit.

Field Name	Description
Frequency	The specific duration for which the limits can be utilized and available. The options are: • Daily • Monthly
Currency	The currency to be set for the limit.
Cumulative Transaction Amount	The collective amount in selected currency for transactions that can be performed in a day.
Maximum Transactions	The maximum number of transactions that can be performed per day.

To create a cumulative limit:

1. Click the **Cumulative** tab. The **Limits Definition - Create** screen with **Cumulative** tab appears.
2. Enter the relevant information in **Limit Code** and **Limit Description** field.
3. From the **Frequency** field, select the appropriate duration for the limits.
4. From the **Currency** field, select the appropriate currency for the limits.
5. In the **Cumulative Transaction Amount** field, enter the collective amount of transaction in local currency.
6. In the **Maximum Transactions** field, enter the value for maximum number of transactions.
7. Click **Save** to save the created limit.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction and navigate back to dashboard.
8. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
9. The success message of transaction submission appears.
   Click **OK** to complete the transaction.

Limits Definition - Cooling Period – Create



Field Description

Field Name	Description
Limit Type	The type of limit. The limit type for selection are: • Transaction – It is the initiation limit with minimum and maximum amount • Cumulative – It is a duration based limit with maximum amount and number of transactions for a day/month • Cooling Period – Payee cooling period limit is a time and the amount limit set by the bank during which fund transfer is not allowed or allowed till the specified limit, to a newly added payee.
Limit Code	The name of the limit with unique identifier.
Limit Description	Description of the limit.
Currency	The currency to be set for the limit.
From Time	The cooling period start time. It can be in days and/or hours and/or minutes For example a new payee will be 'active' after a cooling period of 0 days & 0 hours & 30 minutes

Field Name	Description
To Time	The cooling period end time. It can be in days and/or hours and/or minutes. For example a new payee will be 'active' after a cooling period of 0 days & 0 hours & 30 minutes.
Cumulative Transaction Amount	The collective transaction amount in selected currency for a defined cooling period.

To set up multiple amount and time limit slabs:

1. Click the **Cooling Period** tab. The **Limits Definition -** Create screen with Cooling Period tab appears.
2. Enter the relevant information in **Limit Code** and **Limit Description** field.
3. From the **Currency** field, select the appropriate currency for the limits.
4. From the **From Time** and **To Time** field, select the appropriate day, hours and minutes.
5. In the **Cumulative Transaction Amount** field, enter the collective amount that is applicable for the defined cooling period.
6. Click **Add Time Period** if you want to create more than one amount and time limit slabs.
7. Click **Save** to save the created limit.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction and navigate back to dashboard.
8. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
9. The success message of transaction submission appears.
   Click **OK** to complete the transaction.

Note: You can click to delete a record.

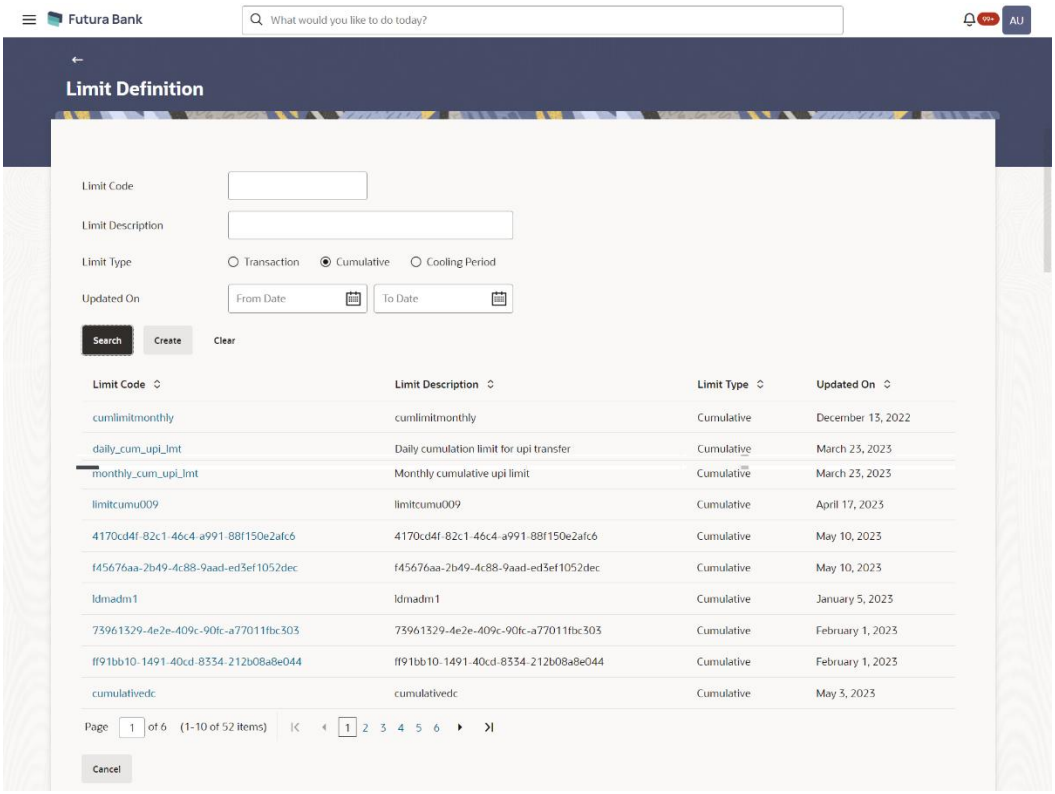
6.3 Limits Definition - Delete Limit

Using this option, System Administrator can delete a limit definition created earlier. Limit definition can be deleted only if it is not in use (available as a part of any limit package).

To delete a limit:

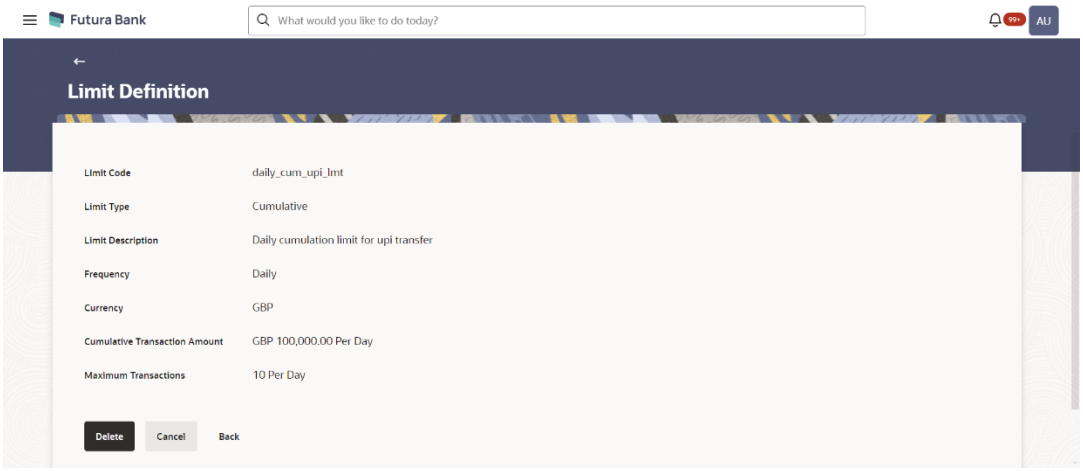
1. In the **Limits Definition** screen, enter the search parameters and click **Search**. The **Limits Definition** screen with search results appears based on the searched criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.

Limits Definition - Search



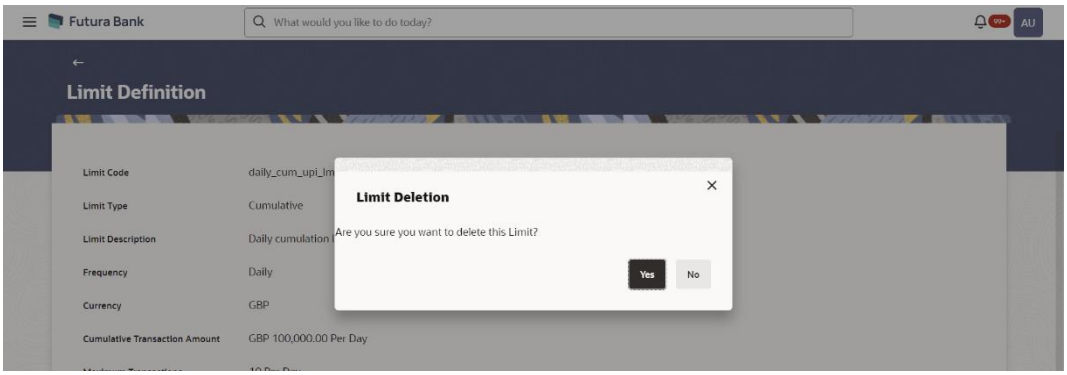
2. Click the **Limit Code** of the record for which you want to view the details. The **Limits Definition -View** screen appears.

Limits Definition - View



3. Click **Delete**. The **Delete Warning** message appears.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction and navigate back to dashboard.

Delete Limit



4. Click **Yes** to confirm the deletion.
   OR
   Click **No** to cancel the deletion process.
5. The success message of transaction submission appears.
   Click **OK** to complete the transaction.

FAQ

1. **Can I delete transaction and/ or cumulative/ cooling period limit definitions against a transaction in limit package?**

No, existing limits against a transaction cannot be deleted; it can only be edited if effective date is starting from a future date.

2. Can I maintain multiple definitions for each limit type?

Yes, you can maintain multiple limit definitions under each limit type.

3. What is a significance of defining different slab limits in case of cooling period limit type?

Payee cooling period limit is a time and the amount limit set by the bank during which fund transfer is not allowed or allowed till the specified limit, to a newly added payee. Administrator can set up 2 or more time slabs to define the payee limits. E.g.

- 0 mins to 30 Mins – Amount limit – $ 0
- 31Min to 60 Mins – Amount limit is $ 5000.

Customer cannot transfer any amount till first 30 mins from the time payee is added. From 31 to 60 mins, customer can maximum transfer upto $ 5000 subject to sufficient transaction and cumulative limits available.

7. Limit Package Management

Limit package is a group of transaction limits. As part of the limit package management, defined limits (created through 'Limit Definition') can be mapped to each transaction or to a transaction group (Created using Transaction Group Maintenance). Each package is associated with a specific channel/Touch point or with a group of Touch points.

A user can be assigned one Retail and multiple Business parties within each entity. Separate limits are applicable for the transaction done by each party.

For Retail Party transactions, the limit package maintained at the user level will be considered and utilized.

For Business Party transactions, the limit package maintained at the party level (as a part of party preference) will be considered and utilized.

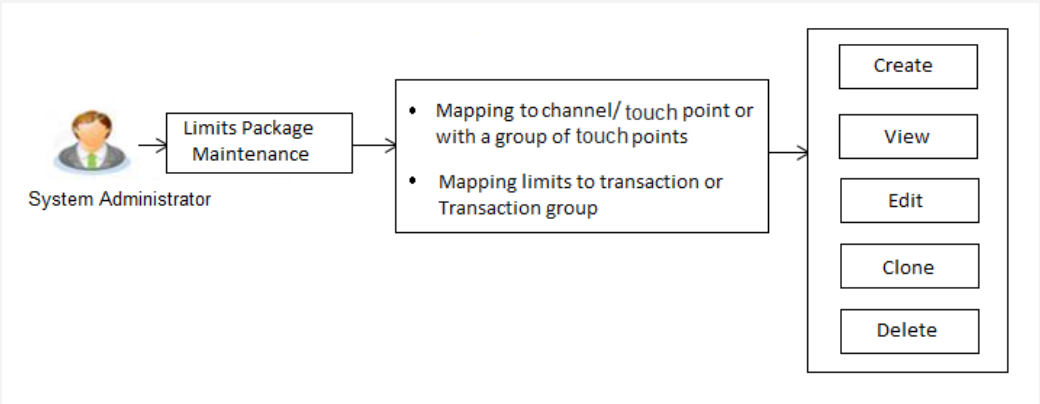
The limits packages once created can be mapped to

- Enterprise Roles (Retail /Corporate/Administrator) – using System Rules
- User Segment – using System Rules maintenance
- Party – using Party Preferences (Cumulative User Limits and Cumulative Customer limits)
- User – using User Management

Prerequisites:

- Transaction access is provided to System Administrator.
- Approval rule set up for System Administrator to perform the actions.
- Transaction aspects - limit parameter is enabled for required transactions,
- Transactions groups are maintained as required.
- Touch Point and touch point groups are maintained as required.
- Limit definitions are maintained.

Workflow



Features supported in application

Following functions can be performed by the bank administrator as part of the limit package maintenance

- Search/ View Limit Package
- Create Limit Package
- Edit Limit Package
- Clone Limit Package
- Delete Limit Package

How to reach here:

System *Administrator Dashboard > Limits > Limit Package Management*
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Limits > Limits Package

7.1 Limit Package Management - View

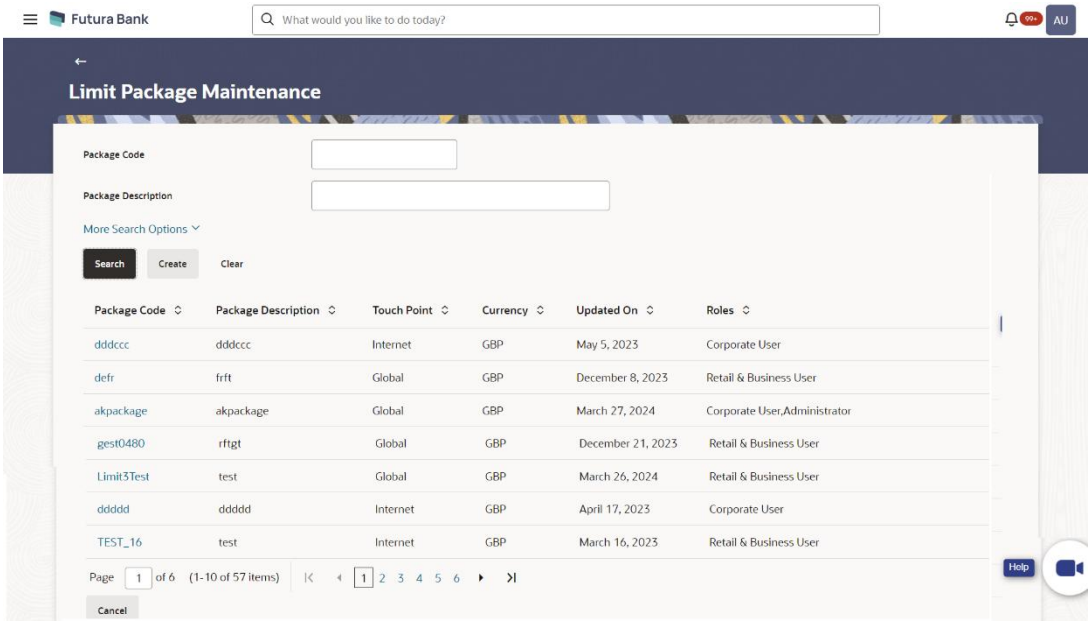
Using this option, Administrator can search for specific limit package based on different search parameters like package code, user segments to for which the package is enabled, touch point/touch point groups to which a package can be mapped etc. The search results displays a list or particular limit package/s based on different search filters selected.

If the search parameters are not specified, records of all the packages maintained in the application are displayed.

To search and view limit package:

1. In the **Limit Package Management** screen, click **Search**. The **Limit Package Management** screen with search results appears based on the searched criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.

Limit Package Management - Search



Field Description

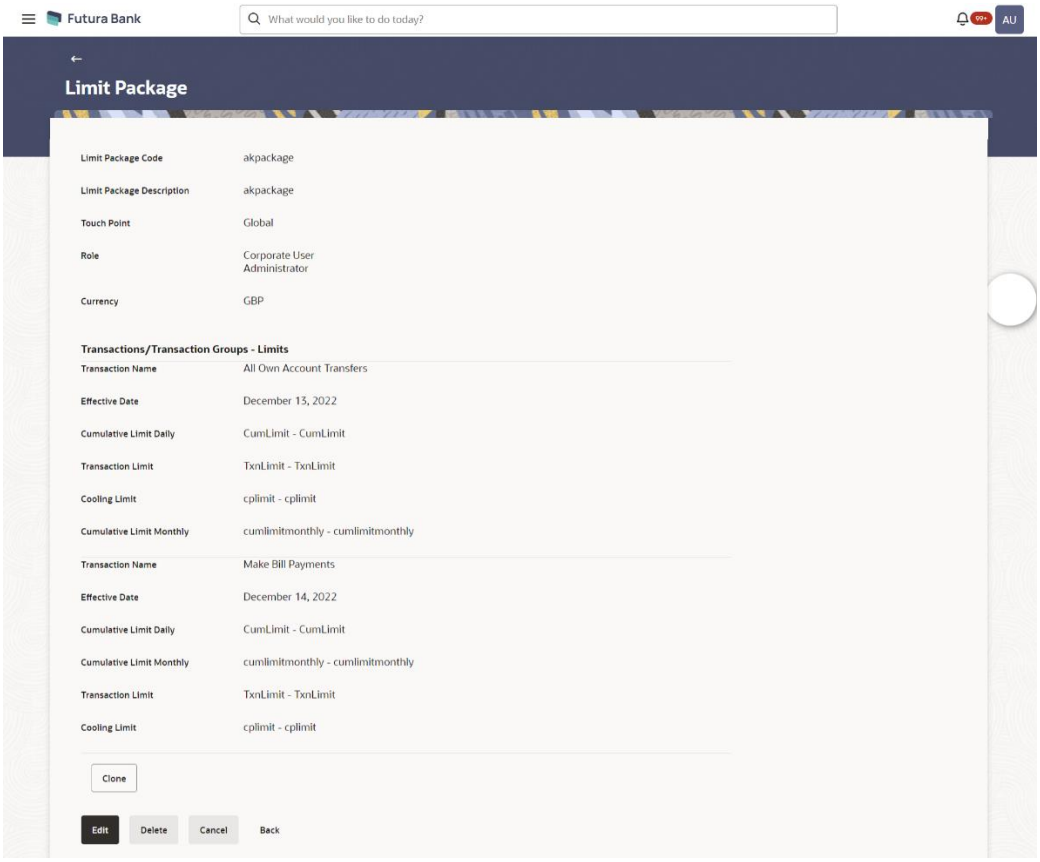
Field Name	Description
Package Code	The unique code assigned to the limit package.
Package Description	Description of the limit package.
Role	The limit is applicable to specific party or role (s).
Touch Point / Group	Name of the touch point or group mapped to a limit package. • Touch Point – To search the limit packages created with specific touch point • Touch Point Group – To search the limit packages created with specific touch point groups which are manually created by an administrator • Global – To search the limit packages created for global group (A group created automatically with all internal and external touch points) of touch points.
Currency	Currency in which the limit package is created.
Updated On	Date range in which limit packages were updated.

Search Results

Field Name	Description
Package Code	The unique code assigned to the limit package.
Package Description	Description of the limit package.
Touch Point	Name of the touch point mapped to a limit package. If package is assigned to specific Touch Point - Touch Point Name is displayed If package is assigned to specific Touch Point Group - Touch Point Group description is displayed If package is assigned to Global Touch Point Group – value 'Global' is displayed on screen.
Currency	Currency in which the limit package is created.
Updated On	Date on which limit package was updated.
Roles	The limit is applicable to specific party or role (s).

2. Click the **Limit Package Code** of the record for which you want to view the details. The **Limits Package Management - View** screen appears.

Limit Package Management - View



Field Description

Field Name	Description
Limit Package Code	The unique code assigned to the limit package.
Limit Package Description	Description of the limit package.
Touch Point/ Touch Point Group	Name of the touch point or group mapped to a limit package.
Roles	The party or role (s) to which limit is applicable.
Currency	Currency in which the limit package is created.
Transactions / Transaction Groups - Limits	

Field Name	Description
Transactions / Transaction Group Name	Name of the transaction group that is mapped to the limit package.
Effective Date	The date from which the limit package is effective for the transaction/transaction group.
Expiry Date	Expiry date of a specific limit linked to a transaction. This field will be displayed only if expiry date is maintained for each transaction.
Cumulative Limit Daily	The daily cumulative limit set for the specific transaction. It displays the limit name and description along with the cumulative transaction amount and transaction count.
Cumulative Limit Monthly	The cumulative limit set for the specific transaction on basis on month. It displays the limit name and description along with the cumulative transaction amount and transaction count.
Transaction Limit	The transaction limit set for the specific transaction. It displays the limit name and description along with the minimum and maximum transaction amount set for the specific transaction.
Cooling Limit	The cooling limit set for the specific transaction. It displays the limit name and description along with the amount and time limit.

3. Click **Clone** to make another limit package with similar details.

   OR
   Click **Edit** to edit the limit package.
   OR
   Click **Delete** to delete the limit.
   OR
   Click **Cancel** to cancel the transaction and go back to Dashboard.
   OR
   Click **Back** to navigate to the previous screen.

7.2 Limit Package Management - Create

An administrator can create a new limit package using this maintenance. User has to define touch point or a touch point group and a currency in which a package is to be created. The touch points and groups defined are listed for selection. An administrator can also create a limit package for Global Touch point group (a group which is created automatically with all available internal and external touch points) A package can also be enabled for mapping at multiple user segments.

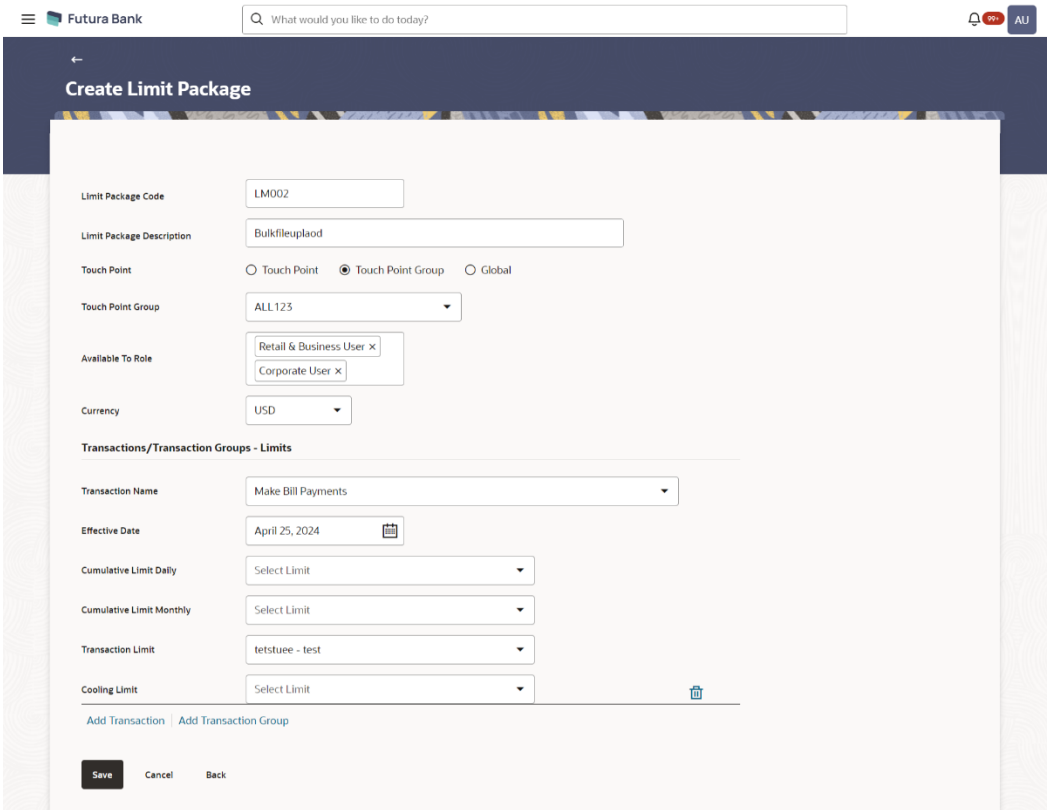
An administrator can add multiple transactions and transaction groups in a package and can assign limit definitions created for each transaction and for a group.

Further, these packages can be assigned at each touch point/group level while defining user segment parameters, party preferences and while creating business users.

To create a limit package:

1. In the **Limit Package Management** screen, click **Create**. The **Limit Package Management - Create** screen appears.

Limit Package Management - Create



Field Description

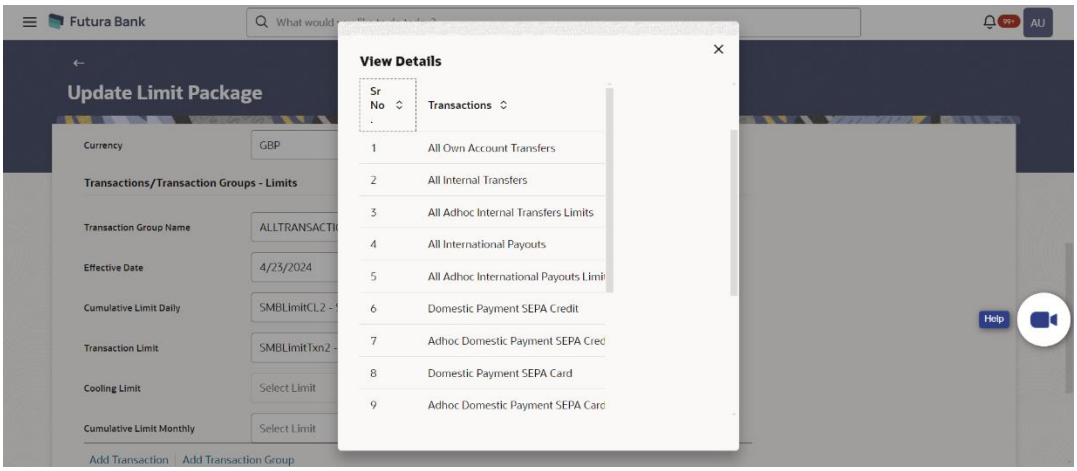
Field Name	Description
Limit Package Code	The unique code of the limit package.
Limit Package Description	Description of the limit package.
Touch Point	Touch point or a group of touch point for which a package is to be created. The options are: • Touch Point • Touch Point Group • Global: This a group of touch points created automatically (default touch point group has all internal and external touch points).
Touch Point	Internal and external touch points defined using touch point maintenance is available for selection. This field is displayed and enabled if you select **Touch Point** option in the **Touch Point** field.
Touch Point Group	Internal and external touch points groups defined using touch point group maintenance are available for selection. This field is displayed and enabled if you select **Touch Point Group** option in the **Touch Point** field.
Available To Role	User segment/s for which a package is to be enabled for mapping.
Currency	The currency to be set for the limit package.
Transactions/ Transaction Group - Limits	
Transactions/ Transaction Group Name	The transaction or transaction group name, to assign the limits to it.
Effective Date	Date from which the limits should be applied for a selected transaction or transaction group.
Cumulative Limit Daily	Cumulative transaction limits which are applicable for each day. All the limit definitions maintained with cumulative – daily limit type and with the same currency as defined at package level are listed for selection.

Field Name	Description
Cumulative Limit Monthly	Cumulative transaction limits which are applicable for each month. All the limit definitions maintained with cumulative – monthly limit type and with the same currency as defined at package level are listed for selection.
Transaction Limit	Transaction minimum and maximum initiation limits. All the limit definitions maintained with transaction – limit type and with the same currency as defined at package level are listed for selection.
Cooling Limit	All the limit definitions maintained with cooling period – limit type and with the same currency as defined at package level are listed for selection.

2. In the **Limit Package Code** field, enter the code for the limit package.
3. In the **Limit Package Description** field, enter the description of the limit package.
4. In the **Touch Point** field, select the appropriate option.
   a. If you select **Touch Point**;
      ii. From the **Touch Point** list, select the appropriate option.
   b. If you select **Touch Point Group**;
      i. From the **Touch Point Group** list, select the appropriate option.
   c. Select **Global**, to create a limit package for a group of all touch points.
5. From **Available To Role** list, select the appropriate role.
6. From **Currency** list, select the appropriate currency to be associated with the Limit Package. It enables the **Transactions / Transaction Group - Limits** section.
7. From the **Transaction / Transaction Group Name** from the list, select the appropriate option for the limit package in the **Transactions / Transaction Group - Limits** section.

Note: Click **View Details** link to view transaction group details.

View Details -Transaction Group Details



Field Description

Field Name	Description
Group Code	Search the transaction groups with group code.
Group Description	Search the transaction groups with group description.
No. of Transactions	Number of transactions associated with the transaction groups.

8. Select the **Effective Date** from the calendar for the limit package in the **Transactions / Transaction Group - Limits** section.
9. From the **Cumulative Limit Daily, Cumulative Limit Monthly, Transaction Limit and Cooling Limit** lists, select the appropriate limits.
10. Click **Add Transaction** and repeat the steps 4 to 6, if you want to assign limits for more transactions.
    OR
    Click **Add Transaction Group** and repeat the steps 4 to 6, if you want to assign limits for more transactions groups.
11. Click **Save** to save the limit package.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate back to previous screen.
12. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate back to previous screen.

13. The success message of transaction submission appears.
    Click **OK** to complete the transaction.

Note: You can click to delete a transaction or cooling limit of a transaction.

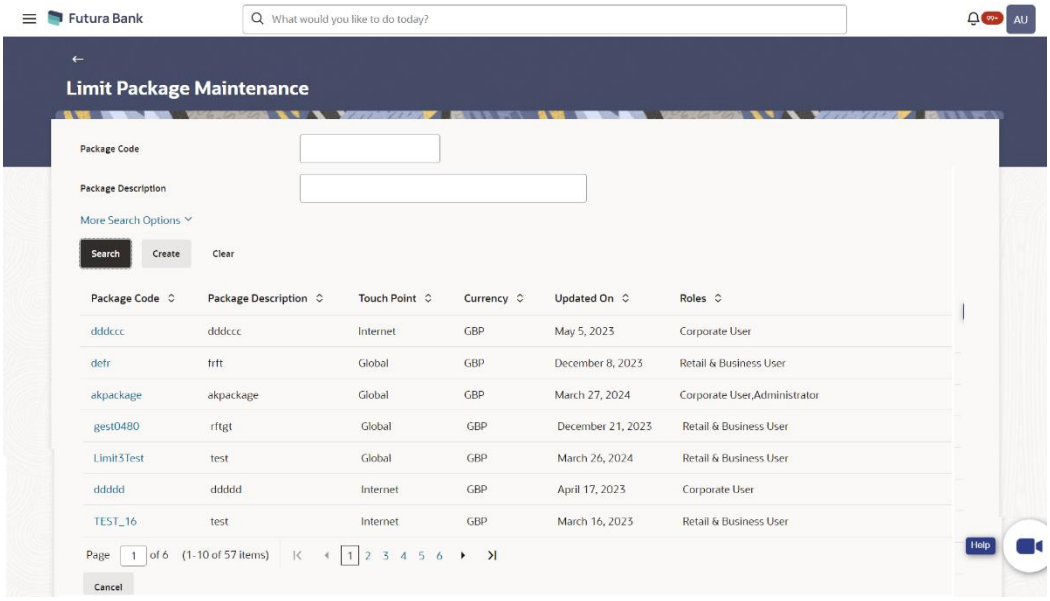
7.3 Limit Package Management - Edit

Using this option, System Administrator can update or edit a limit package created for a specific channel/touch point. User is not allowed to edit the code, currency and touch point details, whereas can add or remove the transactions/transaction groups available as a part of package. And also can edit the limit definitions mapped against each type of limit.

To edit a limit package:

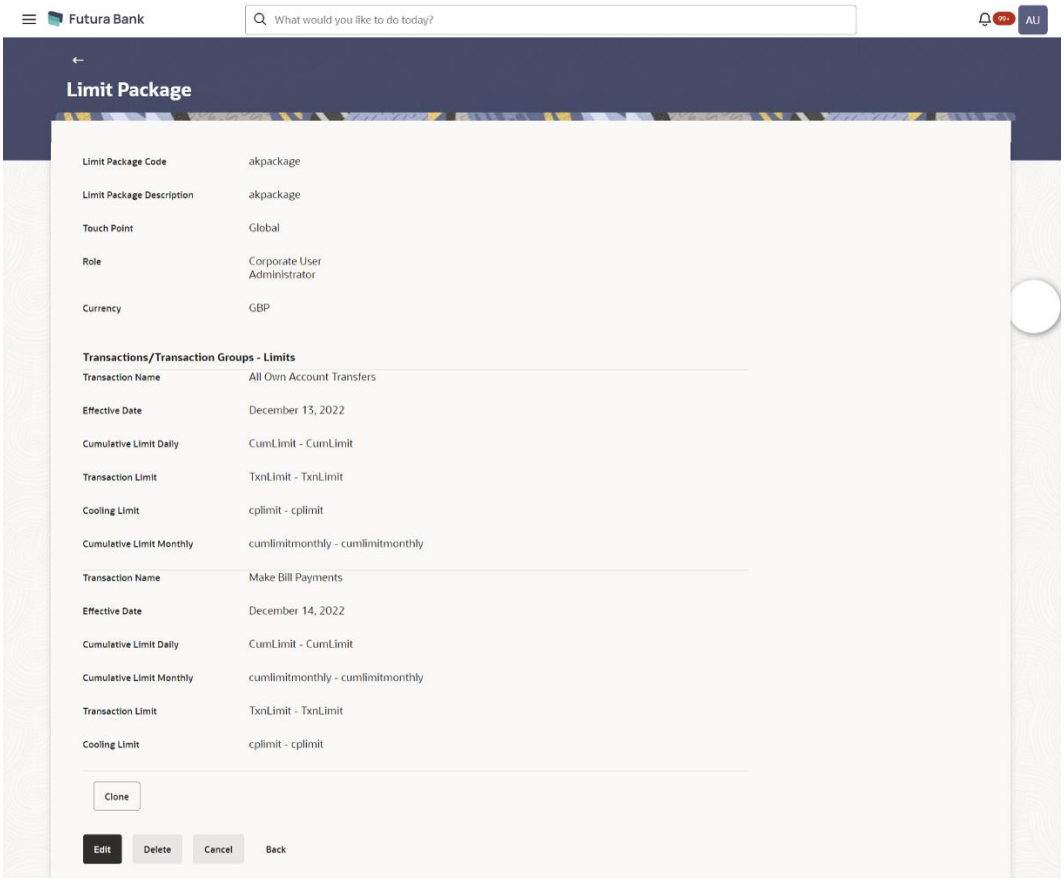
1. In the **Limit Package Management** screen, click **Search**. The **Limits Package Management** screen with search results appears based on the searched criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.

Limit Package Management - Search



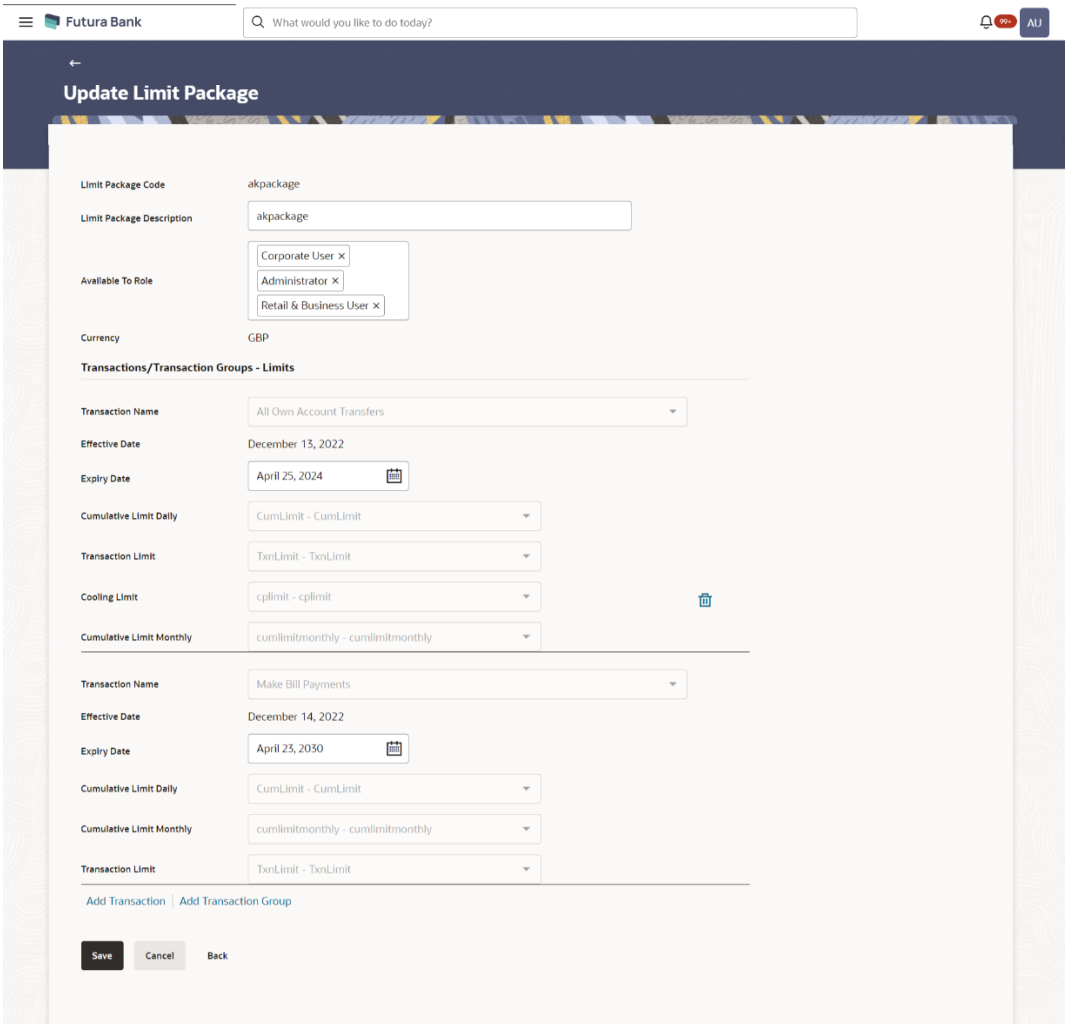
2. Click the **Limit Package Code** of the record for which you want to modify the details. The **Limits Management-View** screen appears.

Limit Package Management – View



3. Click **Edit**. The **Limit Package Management - Edit** screen appears.

Limit Package Management - Edit



Field Description

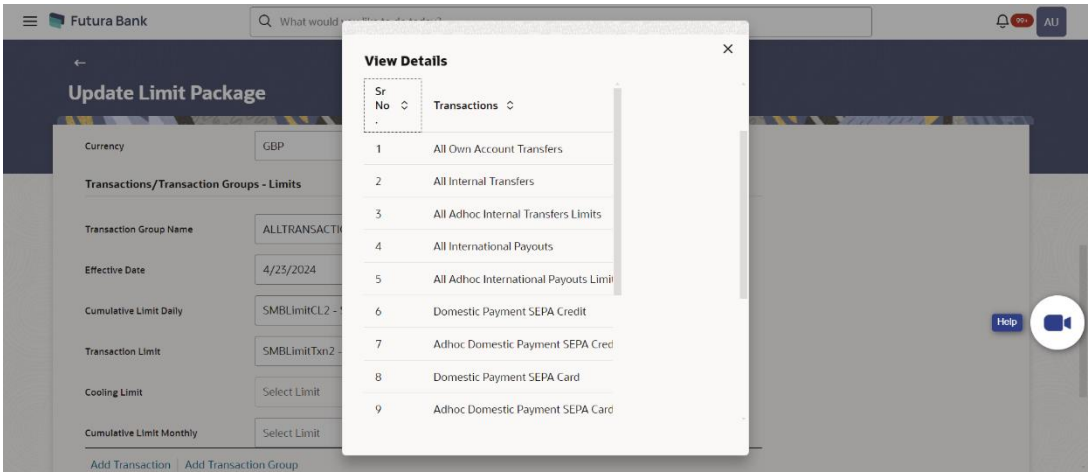
Field Name	Description
Limit Package Code	The unique code of the limit package. This information cannot be edited.
Limit Package Description	Description of the limit package. Details provided previously will be shown in an editable form.
Available To Role	User segment/s for which a package is enabled for mapping. Details provided previously will be shown in an editable form.

Field Name	Description
Currency	The currency which is set for the limit package. This information cannot be edited.
Transactions/ Transaction Group - Limits	
Transactions/ Transaction Group Name	The transaction or transaction group name, to assign the limits to it.
Effective Date	Date from which the limits should be applied for a selected transaction or transaction group.
Expiry Date	Date from which the limits will be deactivated.
Cumulative Limit Daily	Cumulative transaction limits which are applicable for each day. Already assigned package if any is shown in an editable form. All the limit definitions maintained with cumulative – daily limit type and with the same currency as defined at package level are listed for selection.
Cumulative Limit Monthly	Cumulative transaction limits which are applicable for each month. Already assigned limit definition if any is shown in an editable form. All the limit definitions maintained with cumulative – monthly limit type and with the same currency as defined at package level are listed for selection.
Transaction Limit	Transaction minimum and maximum initiation limits. Already assigned definition if any is shown in an editable form. All the limit definitions maintained with transaction – limit type and with the same currency as defined at package level are listed for selection.
Cooling Limit	Already assigned definition if any is shown in an editable form. All the limit definitions maintained with cooling period – limit type and with the same currency as defined at package level are listed for selection.

4. Edit the required details.

Note: Click **View Details** link to view transaction group details.

View Details -Transaction Group Details



Field Description

Field Name	Description
Group Code	Search the transaction groups with group code.
Group Description	Search the transaction groups with group description.
No. of Transactions	Number of transactions associated with the transaction groups.

5. Click **Add Transaction**, if you want to add a new transaction.
   OR
   Click **Add Transaction Group**, if you want to add a new transaction group.
   OR
   Click Delete Transaction to delete an existing transaction/ transaction group.
6. Click **Save** to save the changes made to the limit package.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
8. The success message of transaction submission appears.
   Click **OK** to complete the transaction.

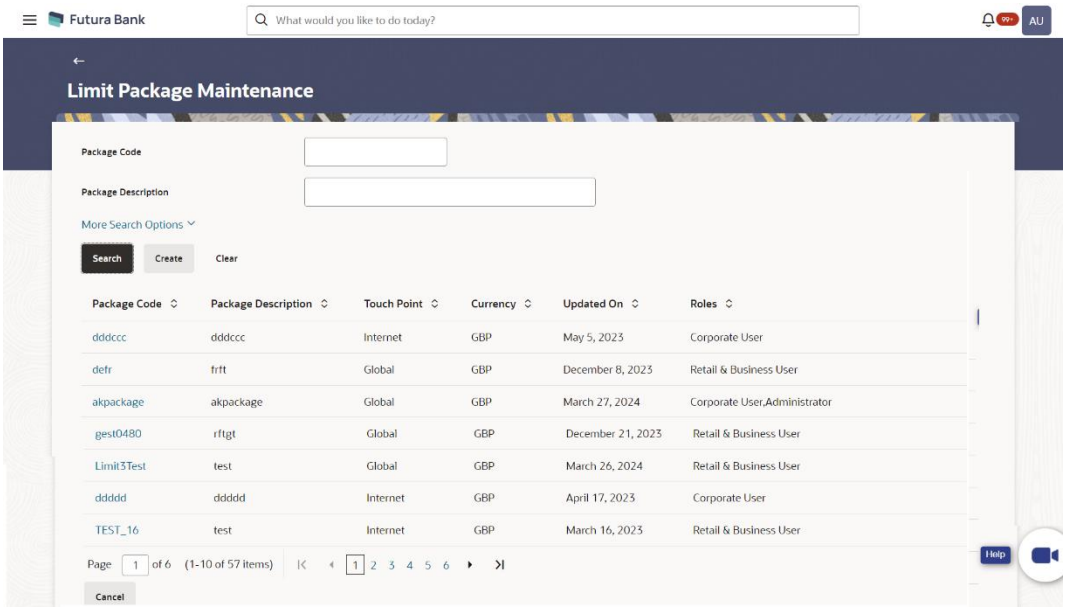
7.4 Limit Package Management - Clone

To speed up the process of creating new limit package, System Administrator can clone an existing limit package. All the values available in an existing package are shown in an editable format, administrator is allowed to make changes in it and save the package with different name.

To clone a limit package:

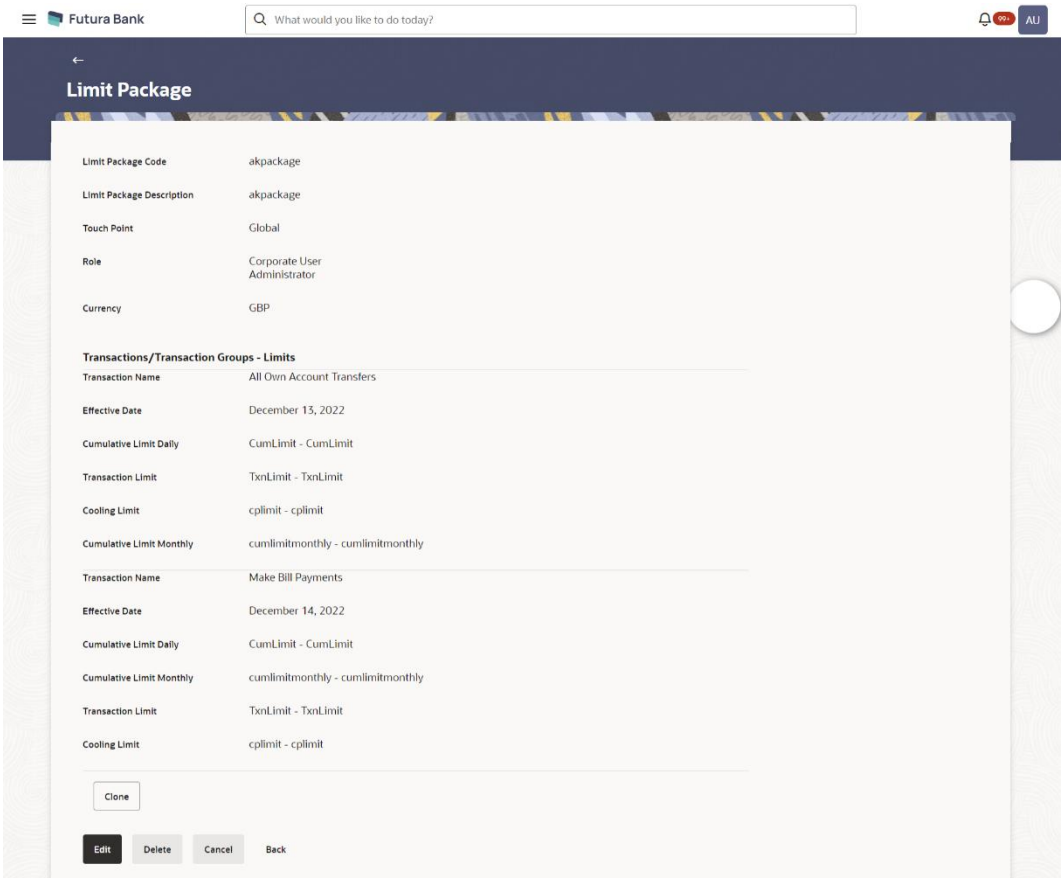
1. In the **Limit Package Management** screen, click **Search**. The **Limits Package Management** screen with search results appears based on the searched criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.

Limit Package Management - Search



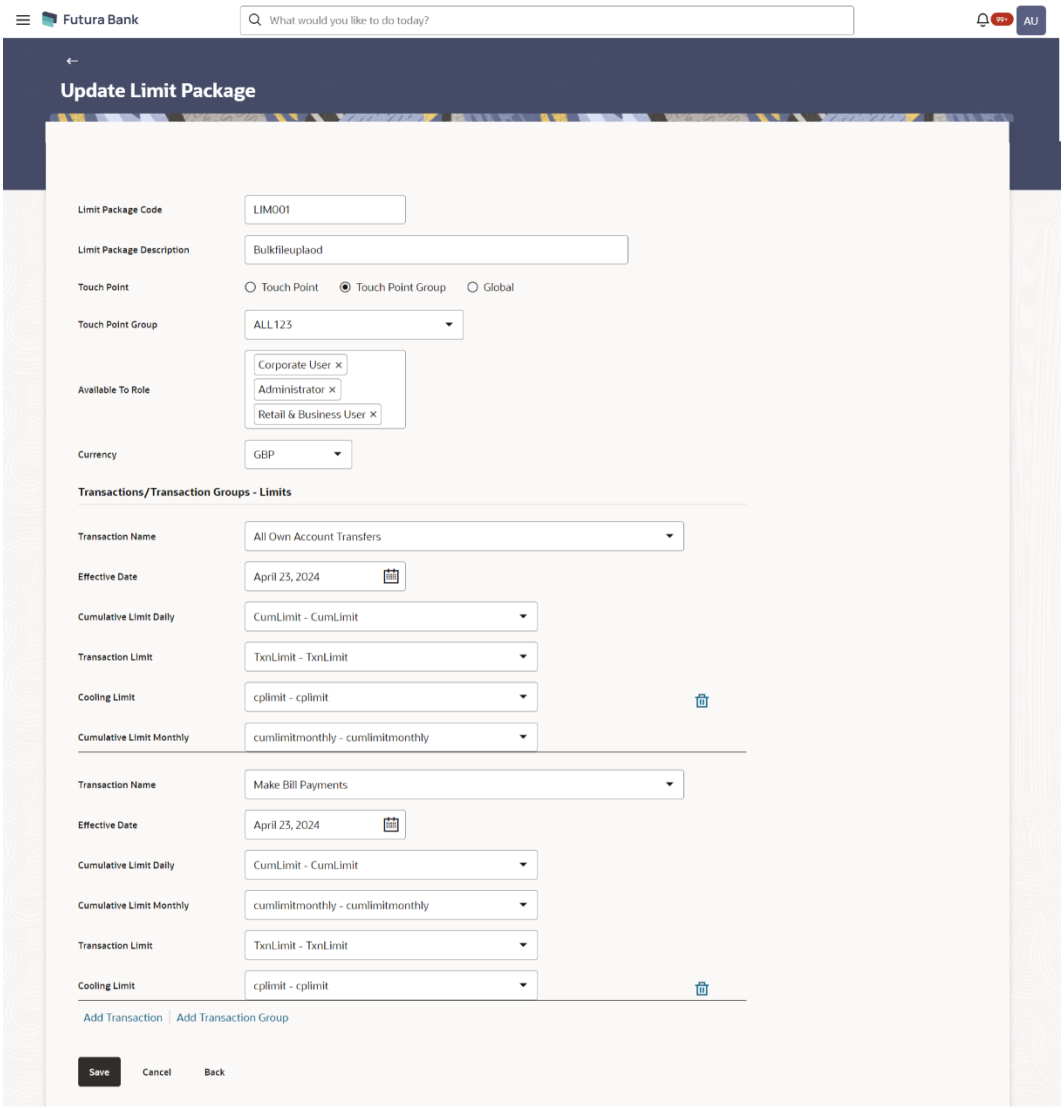
2. Click the **Limit Package Code** of the record for which you want to clone the details. The **Limits Package Management-View** screen appears.

Limit Package Management - View



3. Click **Clone**. The **Limits Package Management - Create** screen appears with existing limit package details.

Limits Package Management - Clone



4. Update limit package with required changes.
5. Click **Save** to save the limit package.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to modify the details.
   The user will be navigated back to the create screen.
   OR
   Click **Cancel** to cancel the transaction.

7. The success message of transaction submission appears.
   Click **OK** to complete the transaction.

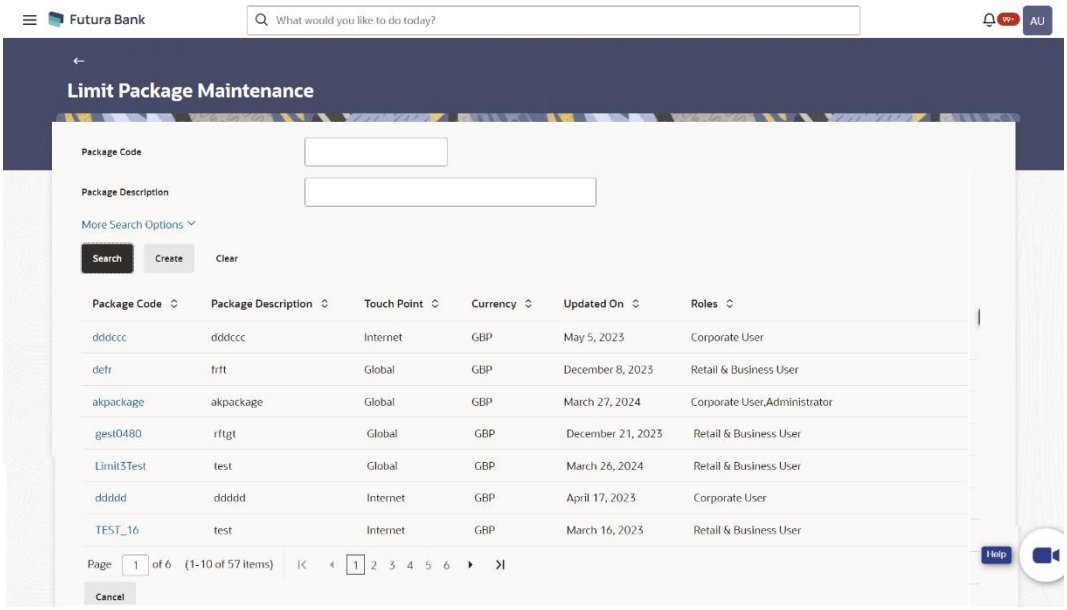
7.5 Limit Package Management - Delete

Using this option, System Administrator can delete a limit package created for a specific channel/ touch point. Deletion of limit package is allowed only if not in use (not mapped at any level)

To delete a limit package:

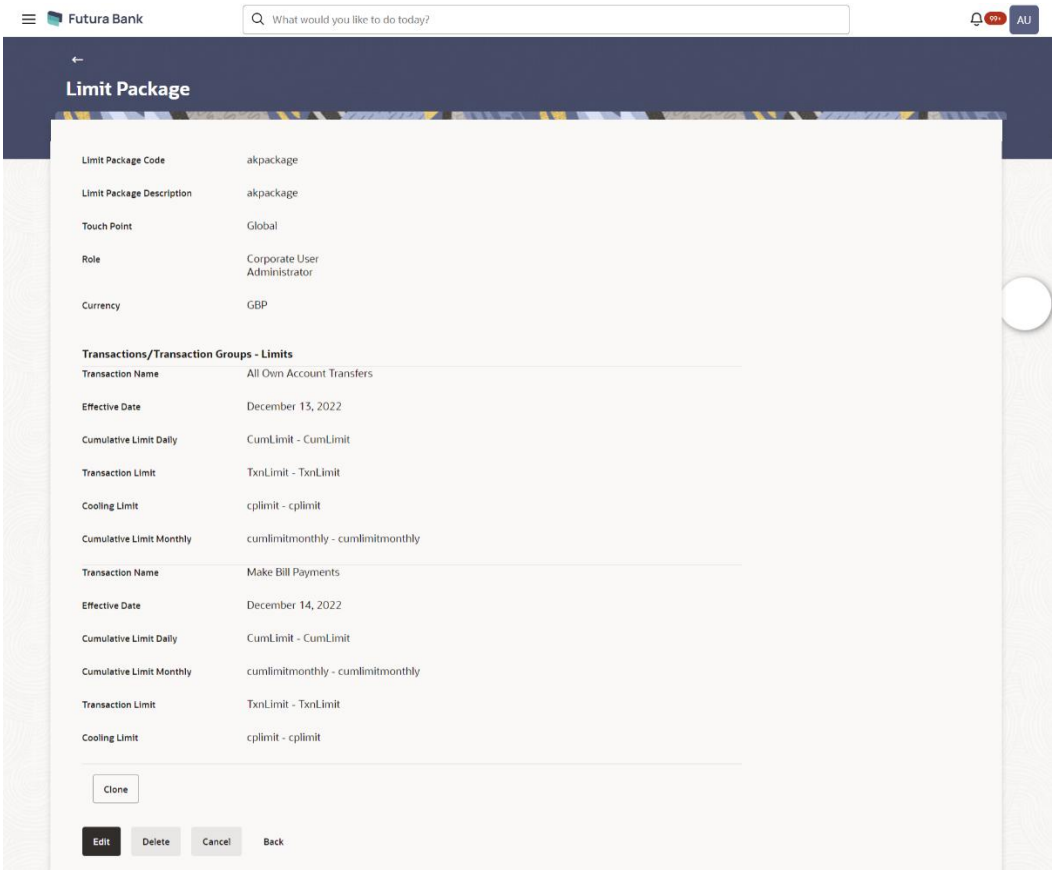
1. In the **Limit Package Management** screen, click **Search**. The **Limits Package Management** screen with search results appears based on the searched criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.

Limit Package Management - Search



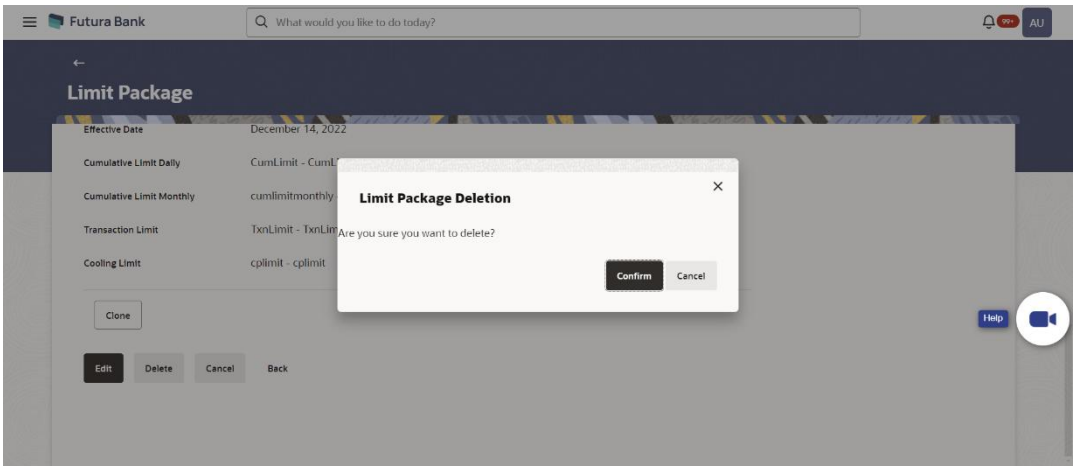
2. Click the **Limit Package Code** of the record for which you want to view the details. The **Limits Package Management-View** screen appears.

Limit Package Management - View



3. Click **Delete**. The **Delete Warning** message appears.

Delete Limit Package



4. Click **Confirm** to confirm the deletion.
   OR
   Click **Cancel** to cancel the deletion process.

5. The success message of limit package deletion appears.
   Click **OK** to complete the transaction.

FAQ

1. **Can I delete transaction and/ or cumulative limits against a transaction in limit package?**

   No, existing limits against a transaction cannot be deleted; it can only be edited if effective date is starting from a future date.

2. I **am unable to delete a limit through limit maintenance?**

   There is a possibility that the limit that you are trying to delete is associated in the limit package against a transaction(s).

3. **I am unable to delete limits package through limit maintenance?**

   There is a possibility that the limit package that you are trying to delete is associated at any of the entities i.e. User / Party / Segment/ Enterprise Role level.

4. **As part of edit, what can I update in the limits package maintenance?**

   You can edit the transaction and/ or cumulative limits against the transaction. You can delete the transaction(s) from the limits package and/or you can also add new transaction(s) as part of the limits package

5. **What is the significance of 'Available to Roles' in Limits package?**

   The roles defined in Limits package will make the package available to the users of that role only.

6. **Have created/ edited/ deleted Limits and/ or Limits package but it is not reflecting in the system even after a successful maintenance save message?**

   There is a possibility that the maintenance is saved but the status is 'Pending Approval'. For the maintenance, if there is an approval required then the changes will reflect only once the approver(s) approve the submitted request.
   If the setup does not require an approval workflow or is self / auto approved, then the same will reflect immediately.

7. **How can I define the touch point groups?**

   A separate menu option 'Touch Point Group Maintenance' is available using which you can maintain internal and external touch point groups.

8. **How can I define the transaction groups?**

A separate menu option ‘Transaction Group Maintenance’ is available using which you can maintain group of transactions.

9. **Can I manually define Global touch point group?**

   No, Touch Point – Global is nothing but a group of all internal and external touch points available in the application. This group cannot be maintained manually,

10. **Will the limits be applicable for newly added touch point or transactions in a respective groups?**

    Yes, limits will also be applicable for transaction or touch points added at a later stage in respective groups which are mapped as a part of limit package.

11. **How the limit will be utilized, if you add a new transaction to the group for which customers have already initiated transactions during the day but before group formation?**

    Limits assigned at individual transaction level will be utilized for the transaction Initiated before the transaction group formation. These limits will not be considered for group limit utilization.

12. **Can I delete a transaction group which is a part of any limit package?**

    No, a transaction group cannot be deleted if a group is already associated with the limit package.

13. **How the limits will be applied if the limit definitions are mapped for a specific transaction and to a group in which the same transaction is available?**

    Limits mapped for a transaction and group will be checked. Only if the sufficient limits are available at both the level, then user will be allowed to perform the transaction.

    Example:

    User level daily transaction limit of Domestic Transfer internet banking channel = 100000

    User level daily transaction limit of Domestic Transfer for mobile banking channel = 50000

    User level daily consolidated touch points transaction limit for Domestic Transfer = 120000

Days	User action	Internet – Touch Point Limit	Mobile – Touch Point limit	Touch Point Group – User level limits
	For internet as a touch point, Domestic Transfer transaction limit assigned by the Bank is 100000.	100000		120000
	For Mobile as a touch point, Domestic Transfer transaction limit assigned by the Bank is 50000		50000	
	This means, user can perform maximum transaction worth 100000 from internet and maximum of 50000 from mobile daily. And touch point group limit maintained is 120000 for a day User level will override the limits defined at user segment/type level			
	1. User preforms Domestic Transfer transaction worth 20000 from mobile touch point. 2. Now, user will be allowed Domestic transfer transaction of 100000 from internet and 30000 from mobile for that day 3. As per touch point group limits, user will be allowed to perform domestic transfer transaction of 100000 from either internet banking OR mobile banking.	100000	30000	100000
	1. User preforms Domestic transfer transaction of 50000 from internet \ on the same day. 2. Now, user will be allowed maximum of 50000 Domestic transfer transaction from internet banking and 30000 from mobile banking for that day. 3. Whereas, as per consolidated touch point limit, user will be allowed to perform Domestic Transfer transaction worth 50000 from either internet or from mobile.	50000	30000	50000
	1. Now user preforms Domestic transfer transaction of 20000 from mobile. 2. Then user will be allowed to perform the transaction of 50000	50000	10000	30000

Days	User action	Internet – Touch Point Limit	Mobile – Touch Point limit	Touch Point Group – User level limits
	from internet and 10000 from mobile for that day. 3. As per consolidated touch point limit, user will be allowed Domestic Transfer transaction of 30000 from either internet or mobile. 4. Now, user will be allowed transaction of 30000 only from internet as consolidated channel limit is reduced to 30000.			
	1. After above transaction, if user utilizes 30000 from internet then internet limit will be 20000 2. Now, if user performs Domestic transfer transaction of any amount from mobile or internet then user will be displayed an error message. As touch point group limits are exhausted.	20000	10000	0.00

8. User Limits

Using this option the System/Bank Administrator can view the current available and utilized limits of specific retail user and also can modify (increase or decrease) the limits as per the requirement.

The user limits can be set for specific transaction level or at transaction group level or for a specific channel or for a group of channels.

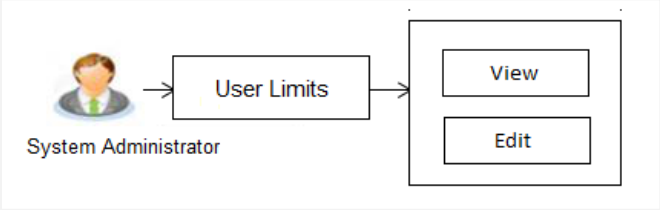
The different types of limits are as follows:

- Daily Count- Permitted number of transactions in a day
- Daily Amount- Cumulative amount of transactions in a day
- Monthly Count- Permitted number of transactions in a month
- Monthly Amount- Permitted number of transactions in a month

Prerequisites:

- Transaction access is provided to System Administrator.
- Limit package are assigned.
- Approval rule set up for System/Bank Administrator to perform the actions.

Workflow



Features supported in application

Following functions can be performed by the System administrator as part of the maintenance:

- Search/ View User Limits
- Edit User Limits

How to reach here:

System *Administrator Dashboard > Limits > User Limits*
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Limits > User Limits

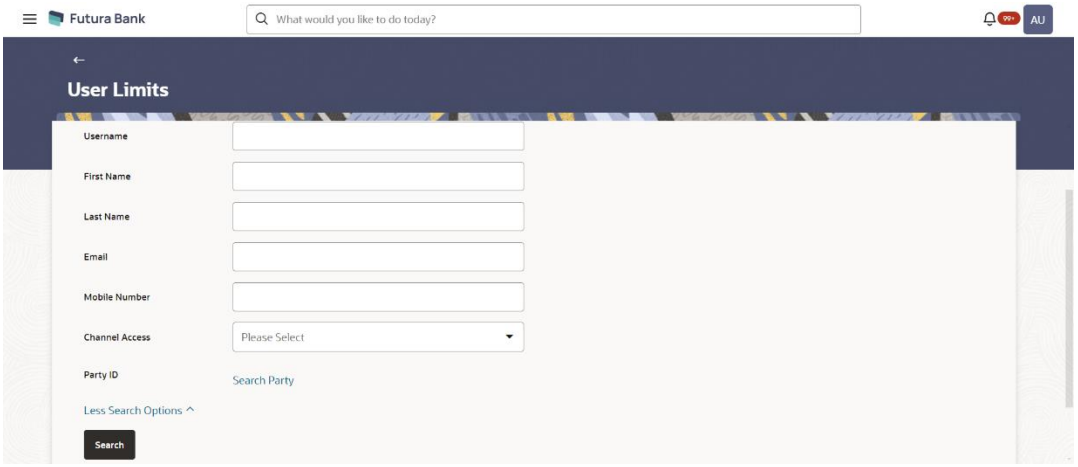
8.1 User Limits - View

Using this option, System Administrator can search and view the current available and utilized limits of specific retail user.

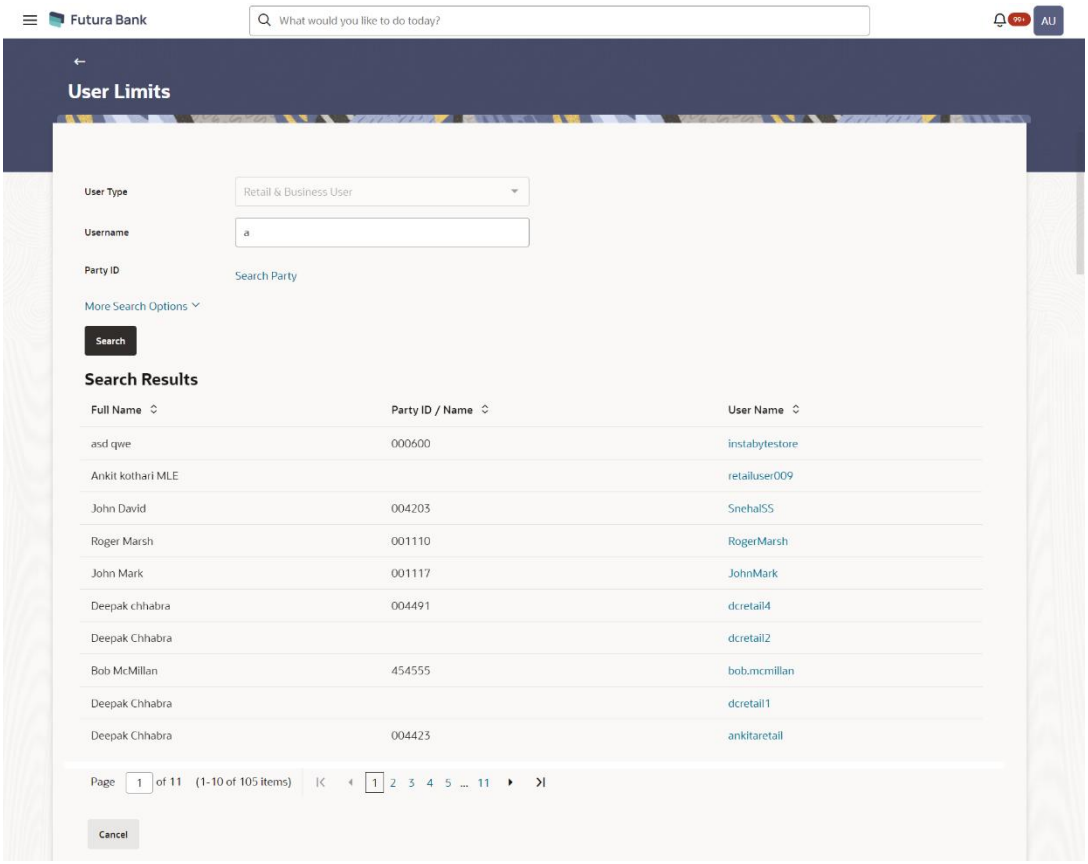
To search and view user limits:

1. Enter the search criteria, click **Search**.
   The search results appear on the **User Limits** screen based on the search parameters.
   OR
   Click **Cancel** if you want to cancel the transaction.
   OR
   Click **Clear** if you want to reset the search parameters.

User Limits - Search



User Limits - Search Result



Field Description

Field Name	Description
User Type	Type of user to be searched. This will be defaulted to 'Retail User'.
User Name	To search the retail user with the user name. Partial search is allowed.

More Search Options

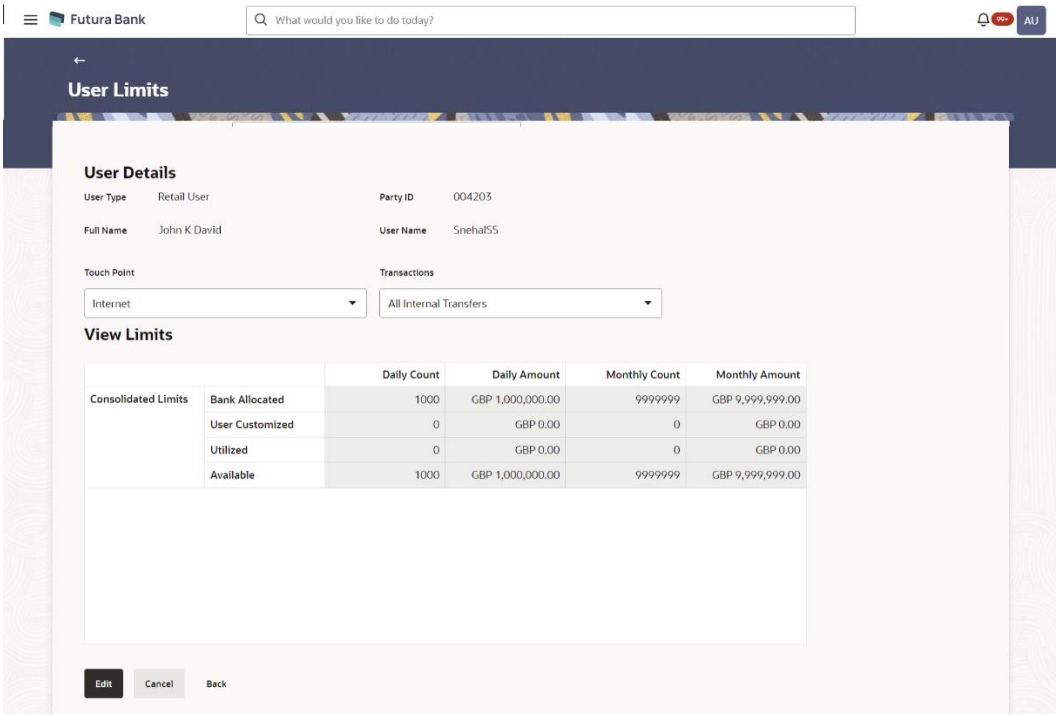
Below fields appears if you click the **More Search Options** link.

First Name	Allows to search based on first name or given name of the retail user.
Last Name	Allows to search based on last name/ surname of the retail user.
Email	Allows to search based on email id of the retail user.

Field Name	Description
Mobile Number	Allows to search based on mobile number of the retail user.
Party ID	Allows to search based on Party id of the retail user.
Search Party Name	
Allows search based on Party name of the retail user.	
Enter Party Name	Party name of the retail user based on which search is to be done.
Search Result	
Full Name	First name and last name of the retail user.
Party ID	Displays the party id of the retail user.
User Name	Displays the retail user's user name.

2. Click the **User Name** of the record for which you want to view the user limits details. The **User Limits - View** screen appears.

User Limits - View



Field Description

Field Name	Description
User Details	
User Type	Type of user whose limits are displayed.
Party ID	Displays the party id of the retail user.
Full Name	First name and last name of the retail user.
User Name	Displays the retail user's user name.
Touch Point	Name of the touch point of which the limits to be inquired. This will be defaulted to 'Internet' whereas User can change the touch point to view specific limits.
Transactions	Name of the transaction of which the limits to be inquired. This defaulted to the 1st transaction available in the drop-down whereas user can change the transaction to view the transaction specific limits.
View Limits	
Transaction Name	Displays the category wise limits allocation for the transaction which is mapped to the retail user. This section will be displayed if a limits package with selected touch point and transaction is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available

Field Name	Description
Transaction Group	Displays the category wise limits allocation for the transaction group which is mapped to the retail user. This section will be displayed if a limit package with selected touch point and a transaction group (which has selected transaction) is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available
Channel Group	Displays the category wise limits allocation for the Transaction - channel group which is mapped to the retail user as per Touch Point / Transaction selected. This section will be displayed if a limit package with touch point group (which has selected touch point) and a transaction is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available
Channel and Transaction Group	Displays the category wise limits allocation for the channel group and transaction group which is mapped to the retail user. This section will be displayed if a limit package with touch point group (which has selected touch point) and a transaction group (which has selected transaction) is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available

Field Name	Description
Consolidated Limits	Displays the consolidated category wise limits (Limits assigned at global level for specific transaction) allocation which is mapped to the retail user as per Touch Point / Transaction selected. This section will be displayed if a limit package with Global touch points and a transaction is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available
Consolidated and Transaction Group	Displays the category wise limits (Limits assigned at global level for group of transactions) allocation for the consolidated and transaction group which is mapped to the retail user. This section will be displayed if a limit package with Global touch points and a transaction group (which has selected transaction) is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available

3. From the **Touch Point** list, select the appropriate option whose user limits to be viewed.
4. From the **Transactions** list, select the appropriate option whose user limits to be viewed.
5. Click **Edit** to edit the user limits.
   OR
   Click **Cancel** to cancel the transaction and go back to Dashboard.
   OR
   Click **Back** to navigate to the previous screen.

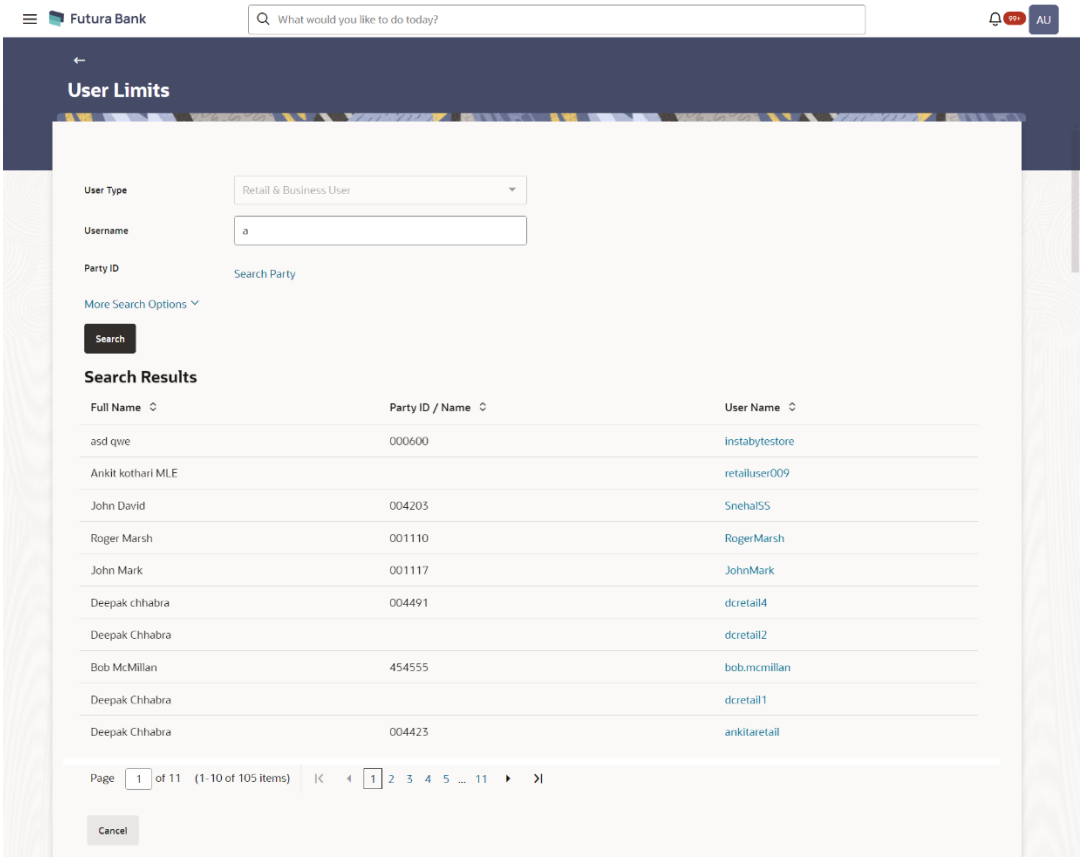
8.2 User Limits - Edit

Using this option, System Administrator can update or edit (increase or decrease) the limits as per the requirement for a specific retail user.

To edit user limits:

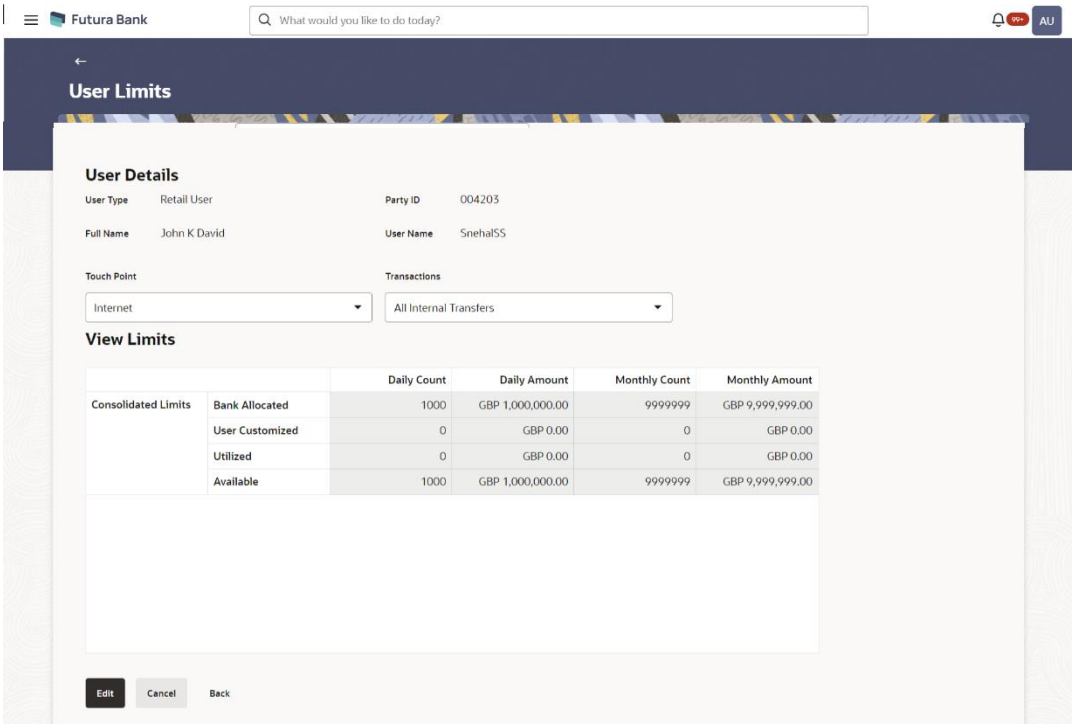
1. In the **User Limits** screen, click **Search**. The **User Limits** screen with search results appears based on the searched criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.

User Limits - Search Result



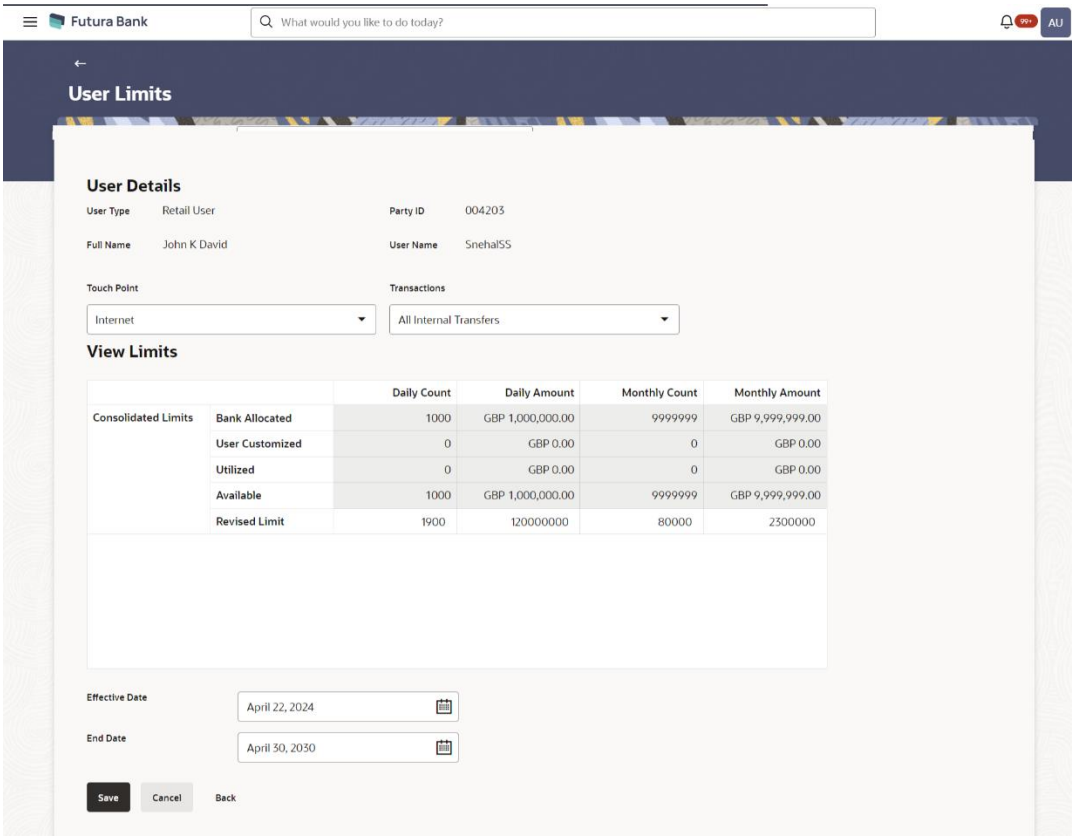
2. Click the **User Name** of the record for which you want to modify the details. The **User Limits-View** screen appears.

User Limits - View



3. Click **Edit**. The **User Limits - Edit** screen appears.

User Limits - Edit



Field Description

Field Name	Description
User Details	
User Type	Type of user whose limits are displayed.
Party ID	Displays the party id of the retail user.
Full Name	First name and last name of the retail user.
User Name	Displays the retail user's user name.
Touch Point	Name of the touch point of which the limits to be inquired.
Transactions	Name of the transaction of which the limits to be inquired.
View Limits	

Field Name	Description
Transaction Name	Displays the category wise limits allocation for the transaction which is mapped to the retail user as per Touch Point / Transaction selected. This section will be displayed if a limits package with selected touch point and transaction is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available • Revised Limits: Specify the new user limit for the transaction. This field is editable.
Transaction Group	Displays the category wise limits allocation for the transaction group which is mapped to the retail user as per Touch Point / Transaction selected. This section will be displayed if a limit package with selected touch point and a transaction group (which has selected transaction) is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available • Revised Limits: Specify the new user limit for the transaction. This field is editable.
Channel Group	Displays the category wise limits allocation for the channel group which is mapped to the retail user as per Touch Point / Transaction selected. This section will be displayed if a limit package with touch point group (which has selected touch point) and a transaction is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available Revised Limits: Specify the new user limit for the transaction. This field is editable.

Field Name	Description
Channel and Transaction Group	Displays the category wise limits allocation for the channel and transaction group which is mapped to the retail user as per Touch Point / Transaction selected. This section will be displayed if a limit package with touch point group (which has selected touch point) and a transaction group (which has selected transaction) is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available • Revised Limits: Specify the new user limit for the transaction. This field is editable.
Consolidated Limits	Displays the consolidated category wise limits allocation which is mapped to the retail user as per Touch Point / Transaction selected. This section will be displayed if a limit package with Global touch points and a transaction is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available Revised Limits: Specify the new user limit for the transaction. This field is editable.

Field Name	Description
Consolidated and Transaction Group	Displays the category wise limits allocation for the consolidated and transaction group which is mapped to the retail user as per Touch Point / Transaction selected. This section will be displayed if a limit package with Global touch points and a transaction group (which has selected transaction) is mapped to the user. The categories are: • Bank Allocated • User Customized • Utilized • Available • Revised Limits: Specify the new user limit for the transaction. This field is editable.
Daily Count	Displays the maximum permitted number of transactions in a day to a retail customer. User can specify the revised daily transaction count limit
Daily Amount	Displays the cumulative amount of transactions in a day for a retail customer. User can specify the revised daily transaction cumulative amount limit.
Monthly Count	Displays the maximum permitted number of transactions in a month to a retail customer. User can specify the revised monthly transaction count limit
Monthly Amount	Displays the cumulative amount of transactions in a month for a retail customer. User can specify the revised monthly transaction cumulative amount limit
Effective Date	The date from which the limit is effective for the transaction. This field is editable.
End Date	End date for the set limits availability on transactions. This field is editable.

4. Click **Edit** to edit the user limits.
   From the **Touch Point** list, select the appropriate option whose user limits to be modified.

From the **Transaction** list, select the appropriate option whose user limits to be modified.
Enter the new values for the limits.
OR
Click **Cancel** to cancel the transaction and go back to Dashboard.
OR
Click **Back** to navigate to the previous screen.

5. Edit the required details.
6. Click **Save** to save the changes made to the user limits.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
8. The success message of limits updation appears.
   Click **OK** to complete the transaction.

FAQ

1. **Can I delete transaction and/ or cumulative group of transactions for which the limits are assigned using this function?**

   No, the transactions and/or group of transactions available in the limit package cannot be deleted or new transaction/transaction group can be added using this maintenance.

2. **Will the changes made in the user's limits will be applicable to all other users whom the same package is mapped?**

   No, the changes made in the limits will be applicable only the user of whom the details are being changed. Other users will continue to enjoy the same limits.

3. **Will the changes made in the user's limits will be effective immediately?**

   The limits will be effective from the date mentioned as 'Effective Date' while updating the limits. If the effective date is current date and day 0 flag is set as 'Next Day' for change in limits applicability. Then the changed limits will be applicable from the next day.

4. **How can I reassure of changing the specific limits, as the screen has lot of information?**

   As a part if user limits change review screen, only the transactions of which the limits are changed are shown on the screen with highlighted values. You can recheck the information and confirm the changes.

5. Can I make the changes in the limits assigned to corporate users?

No, changes cannot be done for the limits assigned to corporate users using this maintenance.

9. Transaction Group Maintenance

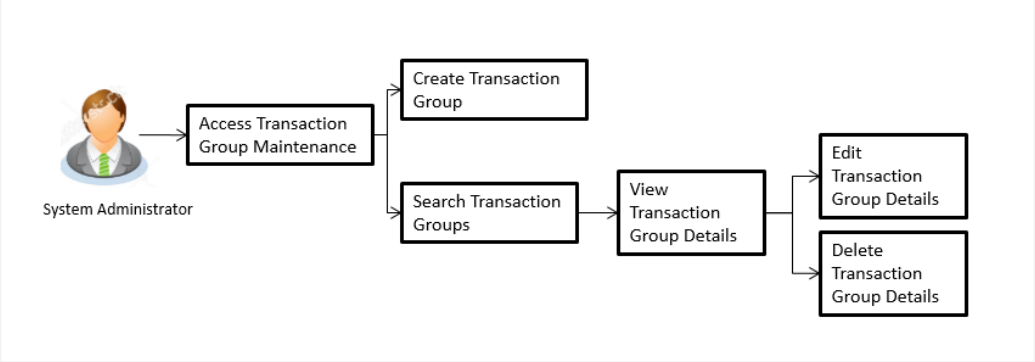
Transaction group maintenance enables the System Administrator to create and maintain group of transactions. Administrator can maintain a transaction group for the purpose of defining consolidated transaction limits. Once limits are assigned at transaction group, these limits acts as collective limit for selected transactions in a group.

For e.g., If the cumulative limit daily (for payment transaction group) is set to GBP 2000, then in a day, customer will be allowed to perform transactions up to GBP 2000 only, spanning across all selected transactions in a group.

Prerequisites:

- Transaction access is provided to system administrator.
- Approval rule set up for system administrator to perform the actions.
- Transactions are available for grouping.

Workflow



Features supported in application

The administrator can perform the following actions:

- Create Transaction Group
- Search/ View Transaction Group
- Edit Transaction Group
- Delete Transaction Group

How to reach here:

System/ Bank Administrator Dashboard > Toggle menu > Menu > Limits > Transaction Group Maintenance

9.1 Transaction Group Maintenance - View

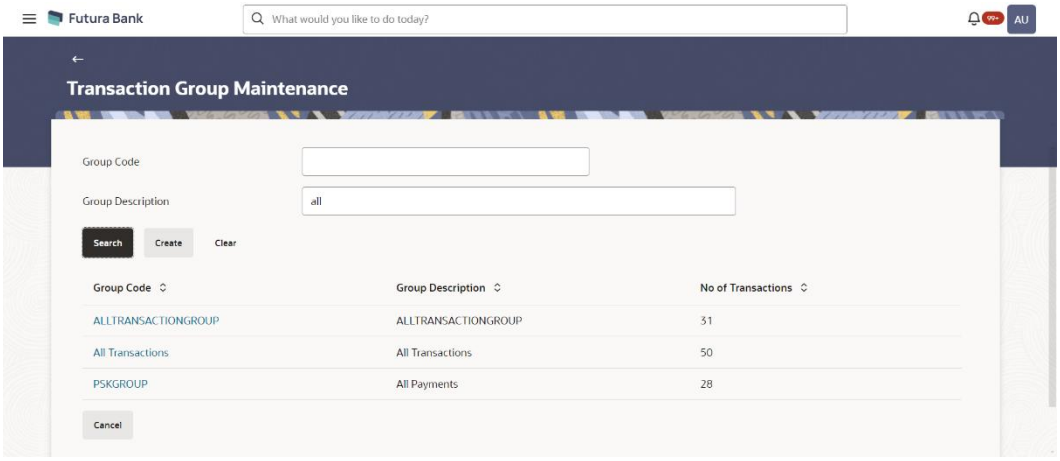
Using this option, System Administrator can search and view details of particular transaction group based on different search parameters like group code or group description. The search results displays a summary of matching transaction groups.

Further, System Administrator can view the details of transaction groups created for the purpose of maintaining limits.

To search and view transaction group:

1. In the **Transaction Group Maintenance** screen, enter the search parameters and click **Search**.
   The **Transaction Group Maintenance** screen with search results appears based on the search criteria.
   OR
   Click **Cancel** to cancel the search process.
   OR
   Click **Clear** to reset the search parameters.

Transaction Group Maintenance - Search



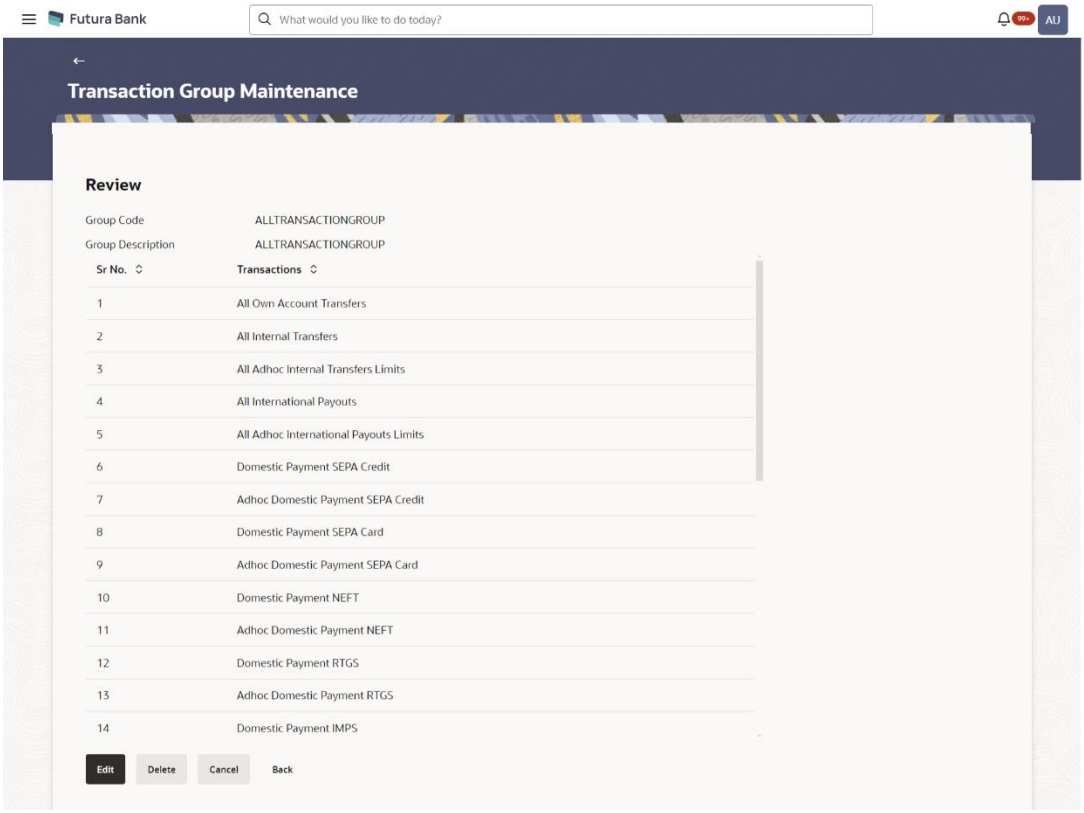
Field Description

Field Name	Description
Group Code	Search the transaction groups with group code.
Group Description	Search the transaction groups with group description.
Search Results	
Group Code	Group code defined for a Transaction Groups.

Field Name	Description
Group Description	Group description defined for a Transaction Groups.
No. of Transactions	Number of transactions associated with the transaction groups.

2. Click the **Group Code** link of the record to view the transaction group details. The **Transaction Group Maintenance - View** screen appears.

Transaction Group Maintenance - View



Field Description

Field Name	Description
Group Code	Group code defined for a Transaction Groups.
Group Description	Group description defined for a Transaction Groups.

Field Name	Description
Transactions	Displays the transactions which are a part of transaction group.

3. Click **Edit** to add or remove the transactions from the transaction group.
   OR
   Click **Delete** to delete the transaction group.
   OR
   Click **Cancel** to cancel the transaction and go back to Dashboard.
   OR
   Click **Back** to navigate to the previous screen.

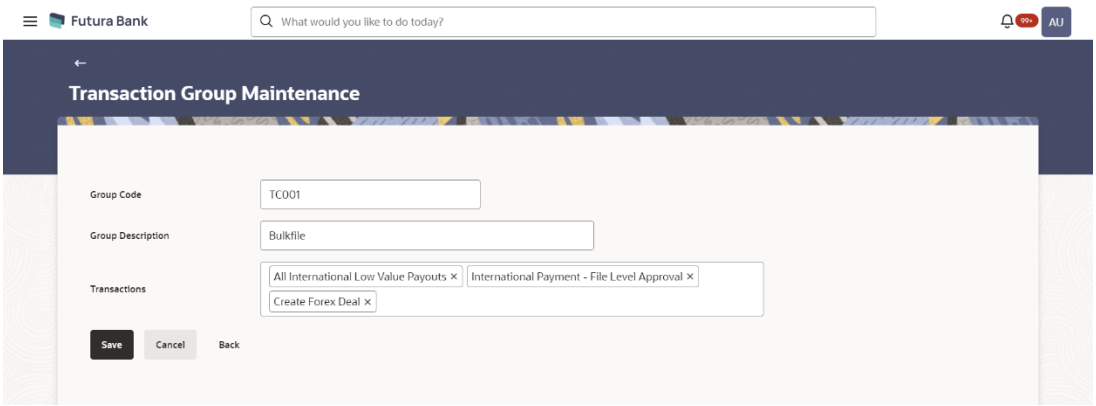
9.2 Transaction Group Maintenance - Create

Using this option, System Administrator can create a new transaction group and can add multiple transactions to a group. Administrator can create multiple transaction groups. Also can add same transactions as a part of multiple groups.

To create a transaction group:

1. In the **Transaction Group Maintenance** screen, click **Create**. The **Transaction Group Maintenance - Create** screen appears.

Transaction Group Maintenance - Create



Field Description

Field Name	Description
Group Code	Unique group code defined for a Transaction Groups.
Group Description	Group description defined for a Transaction Groups.
Transactions	The list of transactions which are a part of transaction group.

2. In the **Group Code** field, enter the code for the transaction group.
3. In the **Group Description** field, enter the description for the transaction group.
4. Click **Select Transactions**, a transaction drop-down appears with the list of transactions grouped according to the type. Multiple transactions can be selected.

Note: All the transactions for which limit flag is enabled will be displayed according to the type.

5. Add required transactions to group.
6. Click **Save** to save the transaction group details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
8. The success message of Transaction Group Maintenance saved successfully appears along with the transaction reference number.
   Click **OK** to complete the transaction.

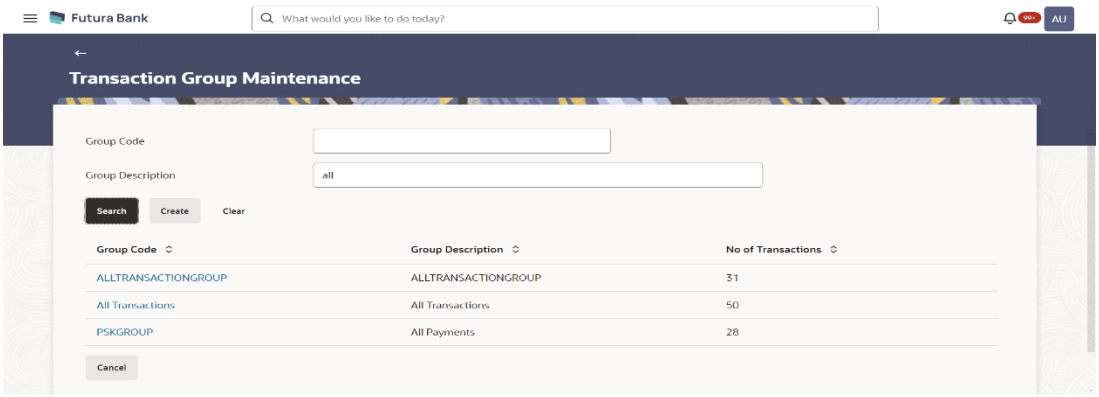
9.3 Transaction Group Maintenance - Edit

Using this option, System Administrator can update or edit a transaction group by adding / removing the transactions associated with the transaction group for purpose of limit maintenance.

To edit a transaction group:

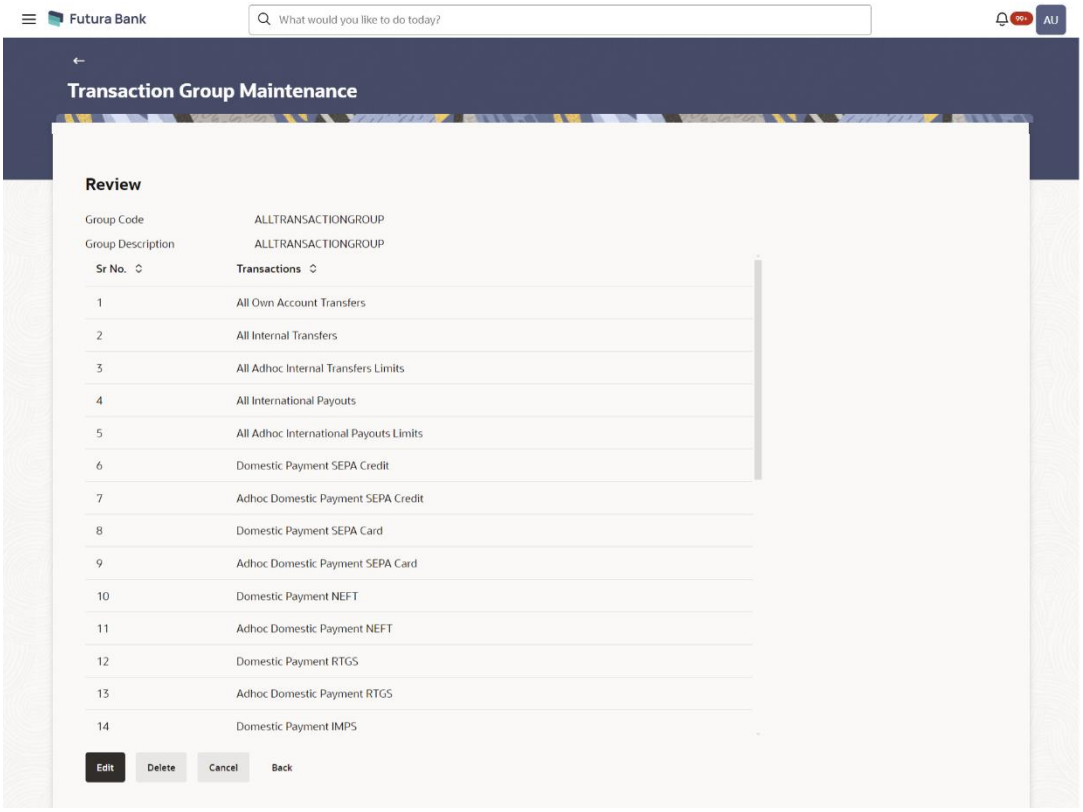
1. In the **Transaction Group Maintenance** screen, click **Search**. The **Transaction Group Maintenance** screen with search results appears based on the searched criteria.
   OR
   Click **Cancel** to cancel the search process.
   OR
   Click **Clear** to reset the search parameters.

Transaction Group Maintenance - Search



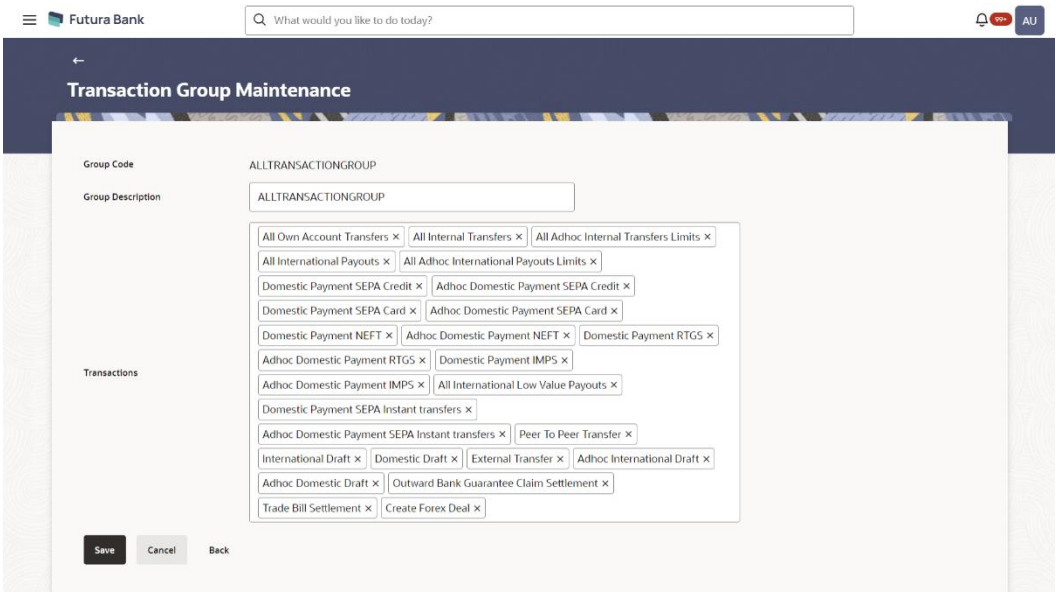
2. Click the **Group Code** link of the record to view the transaction group details. The **Transaction Group Maintenance - View** screen appears.

Transaction Group Maintenance - View



3. Click **Edit** to add or remove the transactions from the transaction group. The **Transaction Group Maintenance - Edit** screen appears.

Transaction Group Maintenance - Edit



4. Edit the required details, e.g. Group Description, Transactions.
5. Clicking transaction area, a transaction drop-down appears with the list of transactions grouped according to the type to add a new transaction.
   OR
   click ✖ to delete an existing transaction from the group.
6. Click **Save** to save the transaction group details
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
8. The success message Transaction Group Maintenance saved successfully appears along with the Transaction reference number.
   Click **OK** to complete the transaction.

9.4 Transaction Group Maintenance - Delete

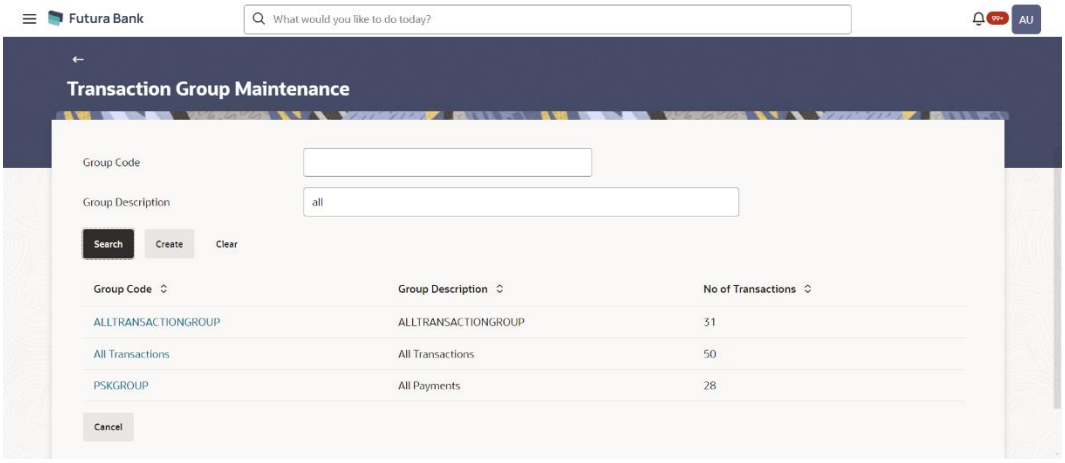
Using this option, System Administrator can delete the transaction group.

Note: System Administrator cannot delete the transaction group, if the limits are associated with that group, and it is mapped to the user/ party which is in use.

To delete a transaction group:

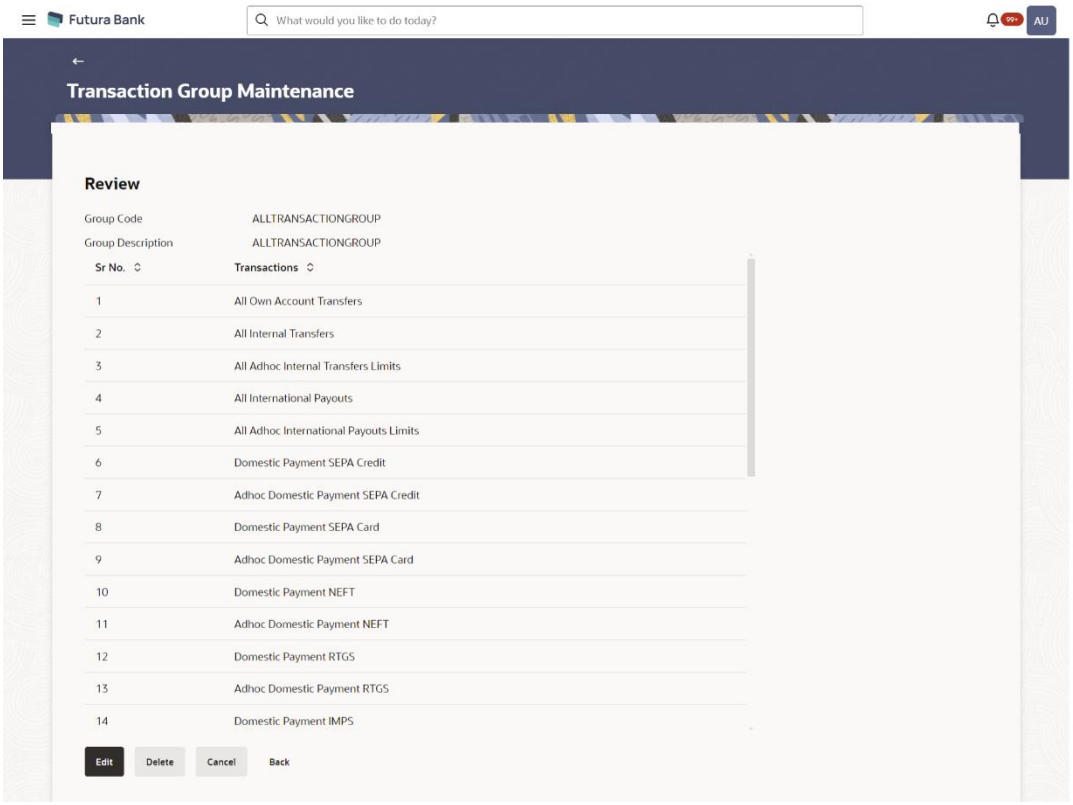
1. In the **Transaction Group Maintenance** screen, click **Search**. The **Transaction Group Maintenance** screen with search results appears based on the searched criteria.
   OR
   Click **Cancel** to cancel the search process.
   OR
   Click **Clear** to reset the search parameters.

Transaction Group Maintenance - Search



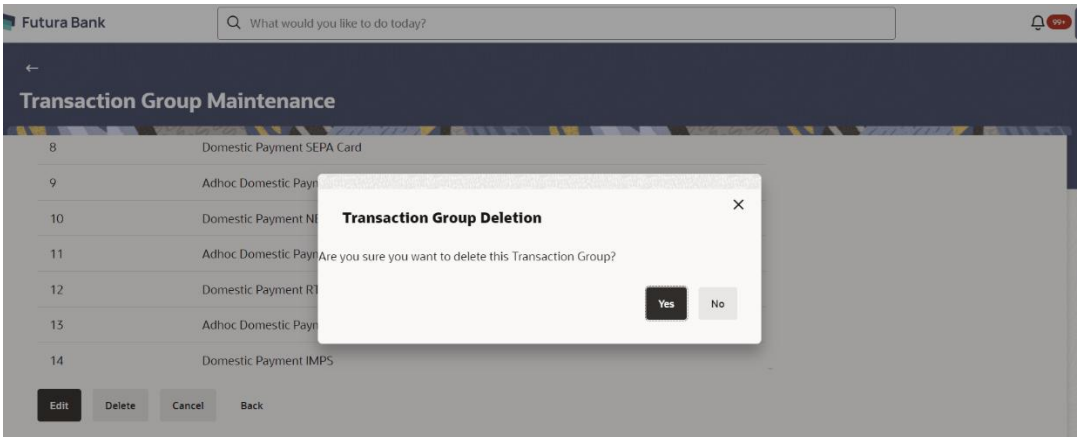
2. Click the **Group Code** link of the record to view the transaction group details. The **Transaction Group Maintenance - View** screen appears.

Transaction Group Maintenance – View



3. Click **Delete**. The **Delete Warning** message appears.

Delete Transaction Group



4. Click **Yes** to confirm the deletion.
   OR
   Click **No** to cancel the deletion process.
5. The success message of transaction group deletion appears.
   Click **OK** to complete the transaction.

FAQ

1. **Can I club one transaction as a part of multiple groups?**

   Yes, one transaction can be clubbed as part multiple groups.

2. **Where can I use these transaction groups?**

   You can define a transaction limits using ‘Limit Package Management’ for these transaction groups.

3. **Can I edit a transaction group which is a part of any limit package?**

   Yes, you can edit the transaction group details if a group is already associated with the limit package.

4. **How the limit will be utilized, if you add a new transaction to the group for which customers have already initiated transactions during the day but before group formation?**

   Limits assigned at individual transaction level will be utilized for the transaction Initiated before the transaction group formation. These limits will not be considered for group limit utilization.

5. **Can I delete a transaction group which is a part of any limit package?**

   No, if a transaction group cannot be deleted if a group is already associated with the limit package.

10. Party Account Access

The System/ Bank Administrator can provide access to accounts held by the party with the bank as available in the core banking application or the respective mid-office application. The system/bank administrator will be able to set up account and transaction access for the Business Parties.

Using this function system administrator can manage access for Current and Savings Accounts, Term Deposit, Loan accounts (Conventional and Islamic) Credit cardsfor a Business party.

Upon navigating to the specific category tab viz. Demand Deposits, Term Deposits, Loans etc., the administrator can select a global check box of 'Map all accounts' to enable all the existing accounts under the selected category for channel banking. If specific accounts are required to be given access then the user needs to select the respective check boxes preceding the account number.

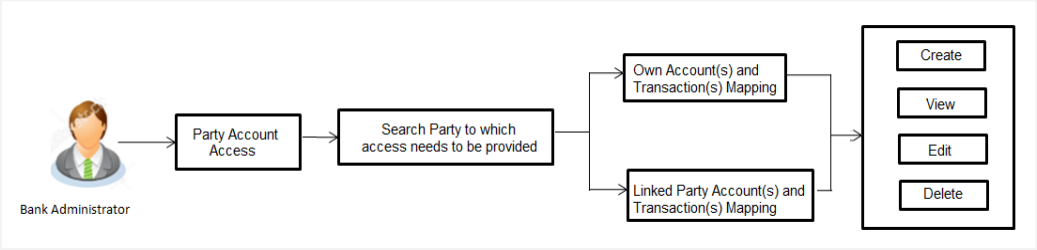
Note: Access Management for Loan Accounts are for accounts fetched from Core Banking System i.e. FCUBS. It is not supported for accounts from Oracle Banking Corporate Loan (OBCL) system.

As part of this maintenance, own accounts and transaction mapping as well as accounts of the linked parties can be mapped to the parent party.

Pre-Requisites

- Party preferences should be created for the party for which access is to be maintained
- Channel Access should be enabled for party for which account access is to be maintained
- Account access maintenance for linked party accounts can be done once there is a party to party linkage maintained.
- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.

Workflow



Features Supported In Application

The following options are available as part of this maintenance:

- Party Account Access - Mapping
- Party Account Access – View
- Party Account Access - Edit

- Party Account Access - Delete

How to reach here:

System/ Bank Administrator Dashboard > Toggle menu > Menu > Access Management > Party Account Access

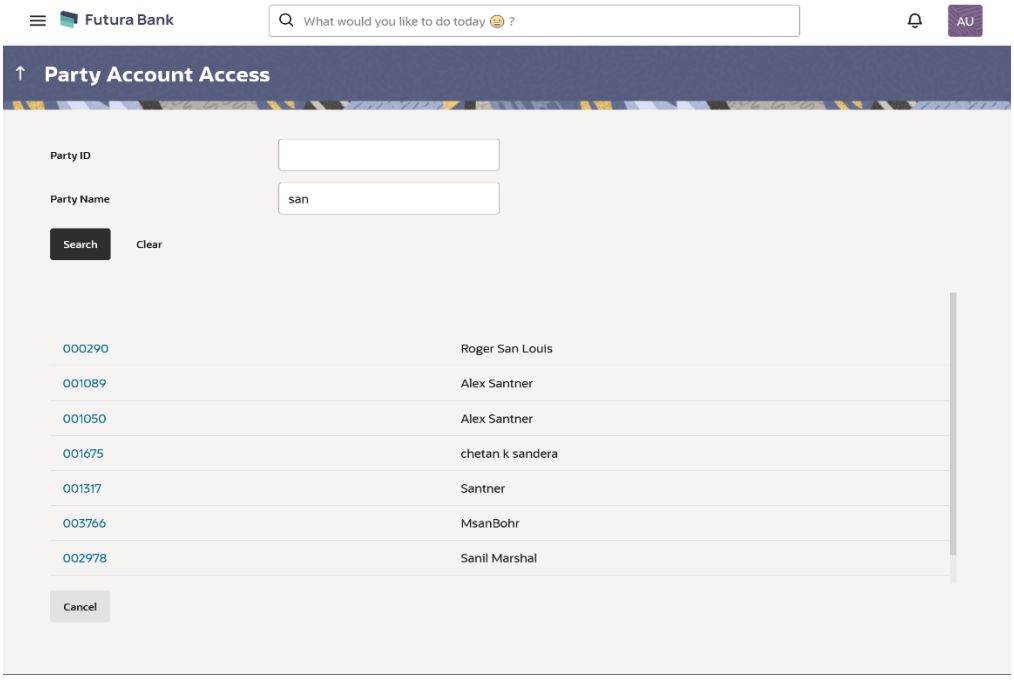
10.1 Party Account Access - Mapping (Create)

The Bank Administrator gets a request with the list of account(s) and transactions for which access needs to be provided to the party.

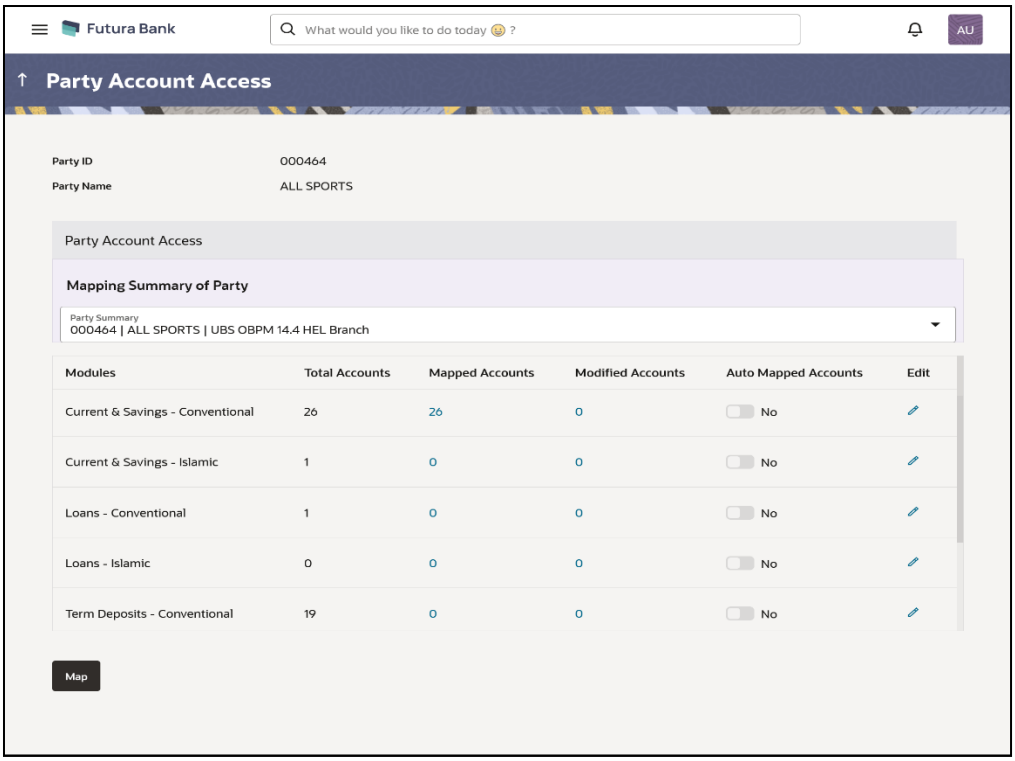
To provide the party with account and transaction access:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**.
   For a searched party, For a searched party, **Mapping Summary of Party** appears.

Party Account Access - Search



Party Account Access - Search Result



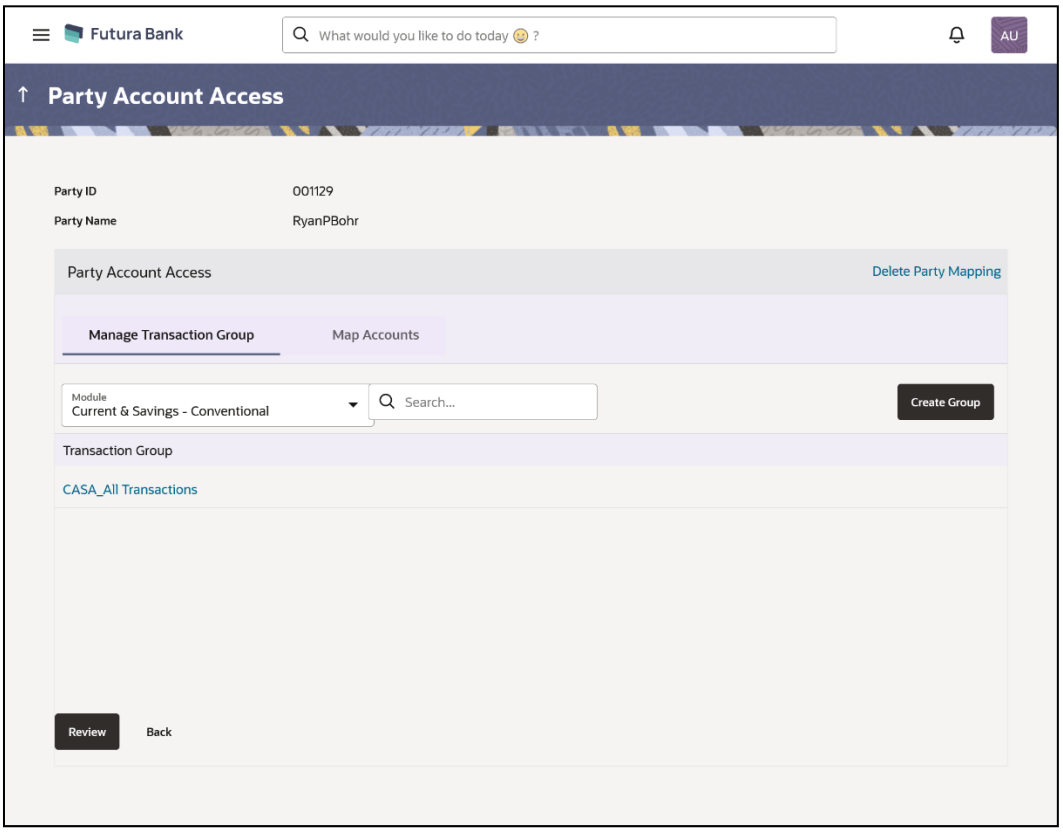
Field Description

Field Name	Description
Modules	Banking Module names.
Total Accounts	Total number of accounts available under the party.
Mapped Accounts	Number of accounts mapped to the particular account type.
Modified Accounts	Number of accounts modified for the particular account type.
Auto Mapped Accounts	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided

Field Name	Description
Edit or Map	Click on the icon next to every module or click on Map button to edit party account access

3. If there is no mapping done for a party, the count for the **Mapped Accounts** will be '**0'**
4. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories i.e. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts
5. Click **Map** or **Edit** (available across each banking module). The **Party Account Access - Create** screen appears.
   OR
   Click **Cancel** to cancel the transaction.

Party Account Access (Create) – Manage Transaction Group tab

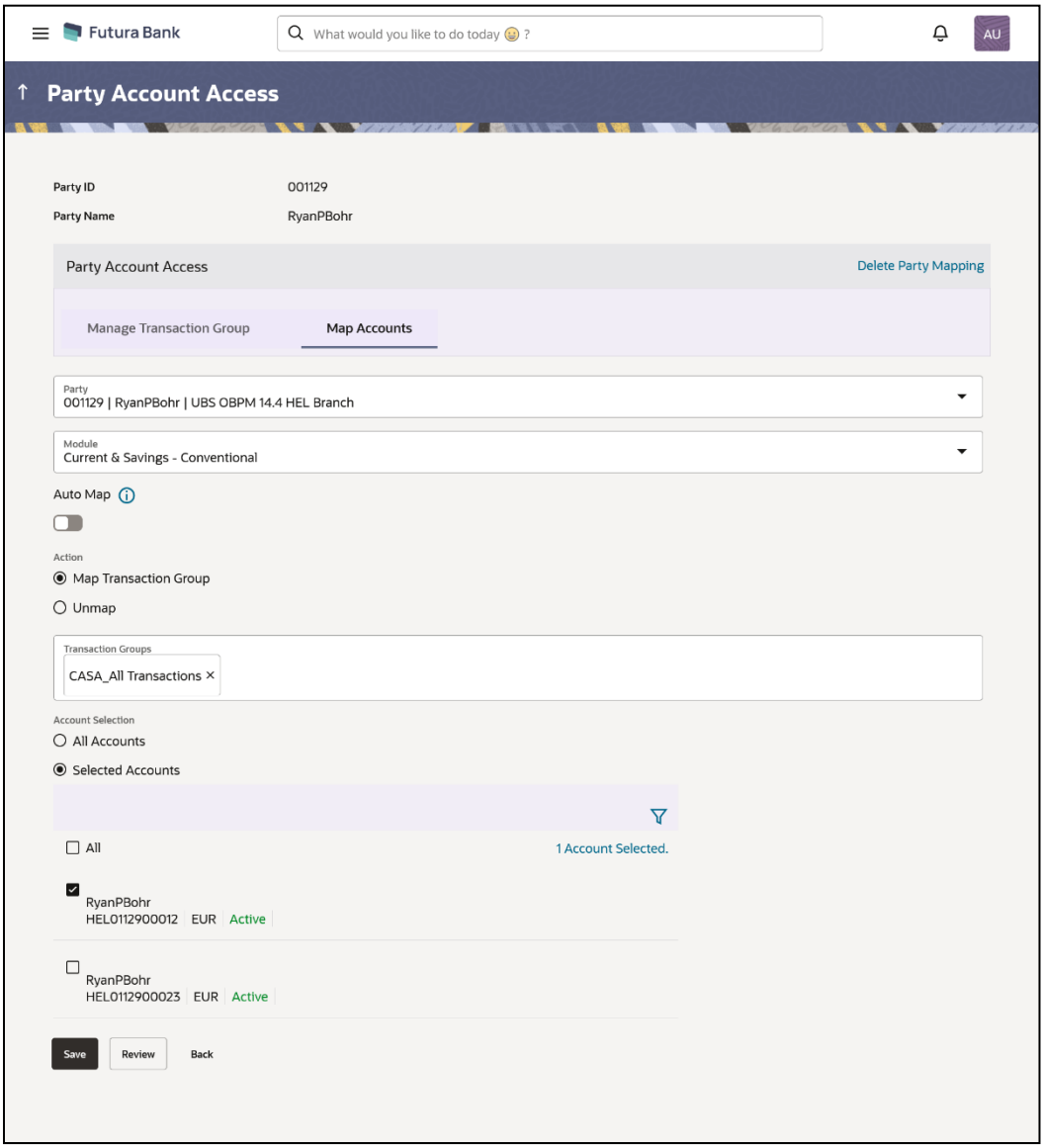


Field Description:

Field Name	Description
Manage Transaction Group tab	
Modules	Select Banking Module to setup account access.
Select Transaction Groups	Select the Transaction group to map transactions and maintaining access in Account Access screens.
Add Transaction Group	Create a new transaction group by clicking the 'ADD' button. Note : • A new group can also be created by cloning/copying an existing transaction group • Multiple transaction groups can be created. • Transaction groups of one Group Corporate will be available for selection only for that Group Corporate

Field Name	Description
Following fields appears in overlay window when user click on **Add** to add new transaction group	
Name of Transaction Group	Specify the new transaction group to map transactions. Click **Verify** to check the availability the specific Transaction Group name.

Party Account Access (Create) – Map Accounts tab



Field Description:

Field Name	Description
Map Accounts tab	
Party	Select the party to map accounts.
Module	Select Banking Module to setup account access.
Auto Map	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided
Action	Select the action to be done for selected transaction group. The options are: • Map Transaction Group: Select Transaction Group, then select the account numbers and then click on Save to map the transaction groups to the selected accounts. Multiple transactions can be mapped • Unmap: Select Unmap option, specify the transaction group to be unmapped and then select the accounts. On clicking Save, the selected transaction group will be unmapped from the account/accounts.. Note: Only one transaction group can be unmapped at a time. A transaction group can be unmapped from All Accounts or Selected Accounts.
Transaction Group	Select one or multiple transaction group/s to be mapped to the selected accounts. Select one transaction group to be unmapped from the selected account/accounts.

Field Name	Description
Account Selection	Select the account numbers to be mapped to the Transaction groups. User can select all the accounts available under selected party ID or click on filter and select the specific accounts. Note : 1) System will show a tag as 'Modified' followed by the transaction group name after the account number. 2) System displays the Account Number along with the Account Name, Account Currency, and Branch Code.
Delete Party Mapping	Click on **Delete Party Mapping** to delete all the Transaction and party account access maintenance done for corporate party all at once

6. The Party Account Access screen has two tabs. Header of the screen shows the Group Corporate Name and Group ID. The manage Transaction Group tab lists down all the **modules, transaction groups** created.
7. Navigate and select specific **module** tab (Including viz. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts, Credit in the first column for which account and transaction access mapping maintenance need to be setup.
8. The user can create a new **transaction group** by clicking the **'ADD'** button. On clicking **Add**, a new overlay will open where all the transactions and inquiries will be listed. User can provide a name the group and select the required transactions and inquiries and click the **save** button.
   OR
   Click **Reset** to clear added details in overlay screen.
9. A new group can also be created by **cloning/copying an existing transaction group**. Once the user selects an existing **transaction group**, system will populate the screen with the transactions selected in the copied group in editable mode. User can select or deselect some of the transactions as per his requirements and create a new group by providing a different transaction group name
10. There will be one factory shipped **Transaction group** for each module, which will have all transactions and inquiries grouped together.

Note: Factory shipped user group cannot be deleted or modified.

11. Once the transaction group/s are created, user can map these transaction groups to one or multiple accounts . Click on **Map Accounts** tab and select Party, then select Transaction Groups, select the account numbers and then click on **Save** to map the transaction groups to the selected accounts.
12. Click on the **Transaction Group link**, to view the list of transactions within the mapped transaction group in an overlay.
13. Select **'All Accounts'** option to map/ unmap transaction groups from all accounts.
    OR
    If specific accounts are required to be mapped, then select the respective check boxes preceding the account number.

14. Once the user maps the accounts, system will show a tag as **'Modified'** followed by the transaction group name after the account number.
15. To map the new accounts, select appropriate option from **Auto Map toggle button**;
    Select **Auto** if you wish to allow access to all future Accounts across banking module.
    OR
    Select **Manual** if you wish to explicitly map new accounts and transactions.
16. User can **unmap** the transaction groups by selecting accounts and then clicking on **Save** button to reset their mapping .
17. User can click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate party in one step.
18. User can drill down his search by applying Filter to search an account basis on the account number, transaction group, account access status, account status and currency
19. The **Review** screen appears. Verify the details, and click **Submit**.
    OR
    Click **Back** to navigate back to previous screen.
20. The screen with success message appears. Click **OK** to complete the transaction.

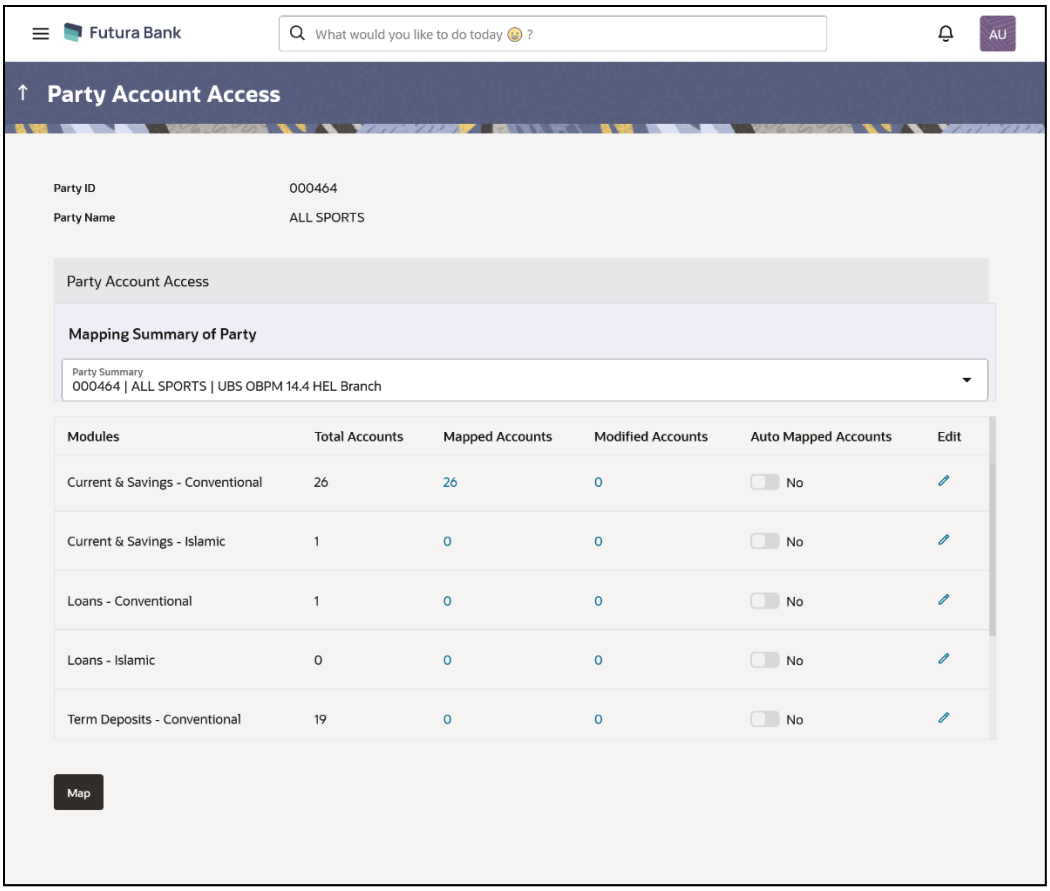
10.2 Party Account Access- View

The Bank Administrator can view the list of account(s) and transactions for which access has been provided to the party.

To Search and view the party account and transaction access:

1. From the **Mapping Summary of Party** drop-down list, select the party id.
2. For a searched party, summary screen will be displayed with total accounts associated with corporate party, status of the accounts mapped for the internet banking, modified accounts if any and Auto account mapping status.
3. Click the link under the total **Mapped accounts** or **Modified accounts**, The **Party Account Access – View** (Transaction Mapping) screen appears. The search result according to the search criteria appears
   OR
   Click **Cancel** to cancel the transaction.

Party Account Access - Summary Results



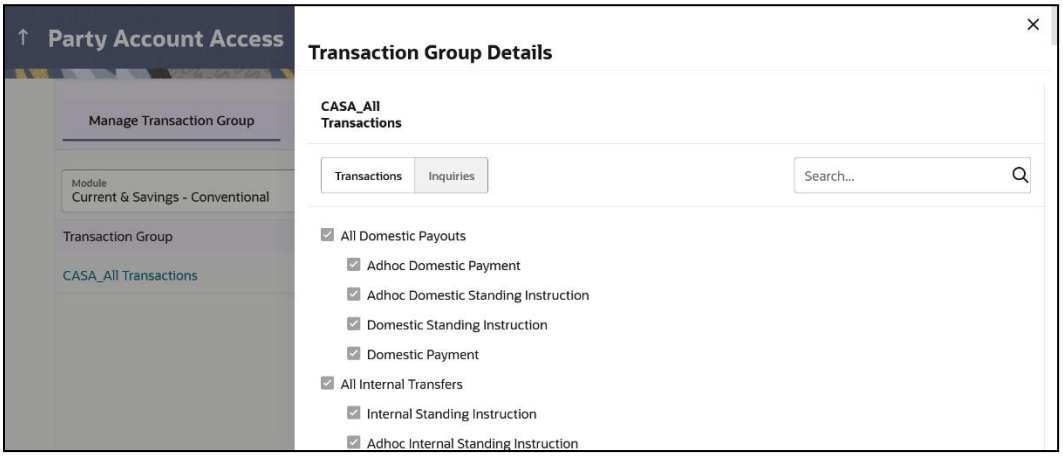
Field Description

Field Name	Description
Mapping Summary of Party	The party for which Party accounts access is being viewed
Modules	Banking Module names.
Total Accounts	Total number of accounts available under the party.
Mapped Accounts	Number of accounts mapped to the particular account type.
Modified Accounts	Number of accounts modified for the particular account type.

Field Name	Description
Auto Mapped Accounts	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided
Edit or Map	Click on the icon next to every module or click on Map button to edit party account access

4. If there is no mapping done for a party, the count for the **Mapped Accounts** will be '**0'**
5. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories

Party Account Access – View



Field Description:

Field Name	Description
Modules	Display name of the product for which account access is being viewed.

Field Name	Description
Mapped Accounts	Display Account number associated with party, and the mapped transaction groups • Display account number along with the name, currency and status of the account as Active or Inactive. The mapped transaction group names can also be viewed against each account
Transaction Groups Details	Display the Transaction group details which are mapped to each account of the selected party. The details of the transaction group includes information related to transactions and inquiries.

6. The Party Account Access details screen has two sections. First column lists down all the Account numbers mapped with the party, including Status of the account (Active or Inactive) and transaction group name
7. In the second column, user can view the **transaction group** details with all the transactions and inquiries access.
8. Click **Cancel** to cancel the transaction.
9. Click **Edit / Map** to update the **Party Account Access** account mapping for new accounts and existing accounts.
   OR
   Click **Cancel** to cancel the transaction.
10. Click **Next** to proceed to the next logical step.
    OR
    Click **Submit** to submit the steps performed so far for approval.
    OR
    Click **Retain Draft** to save the details entered as draft.
    OR
    Click **Cancel** to cancel the transaction.

10.3 Party Account Access- Edit

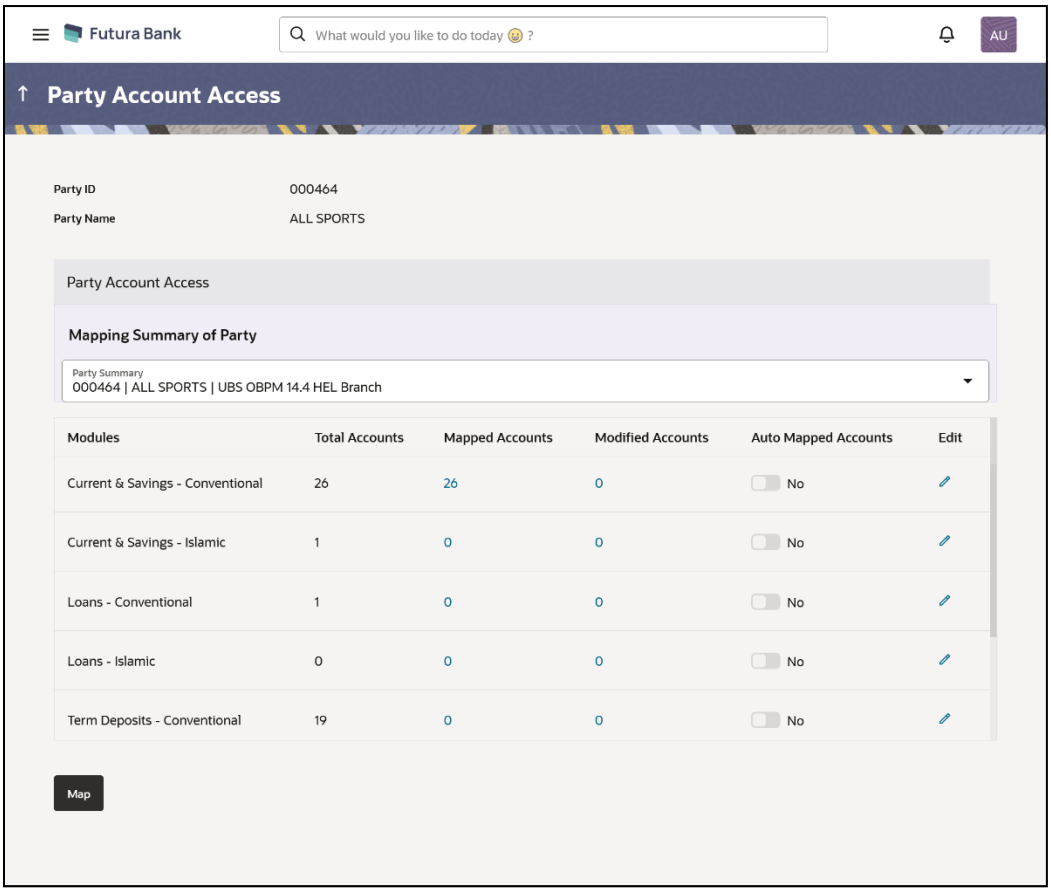
The Bank Administrator gets a request with the list of account(s) and transactions for which access details needs to be edited for the party.

To Search and Edit the party account and transaction access:

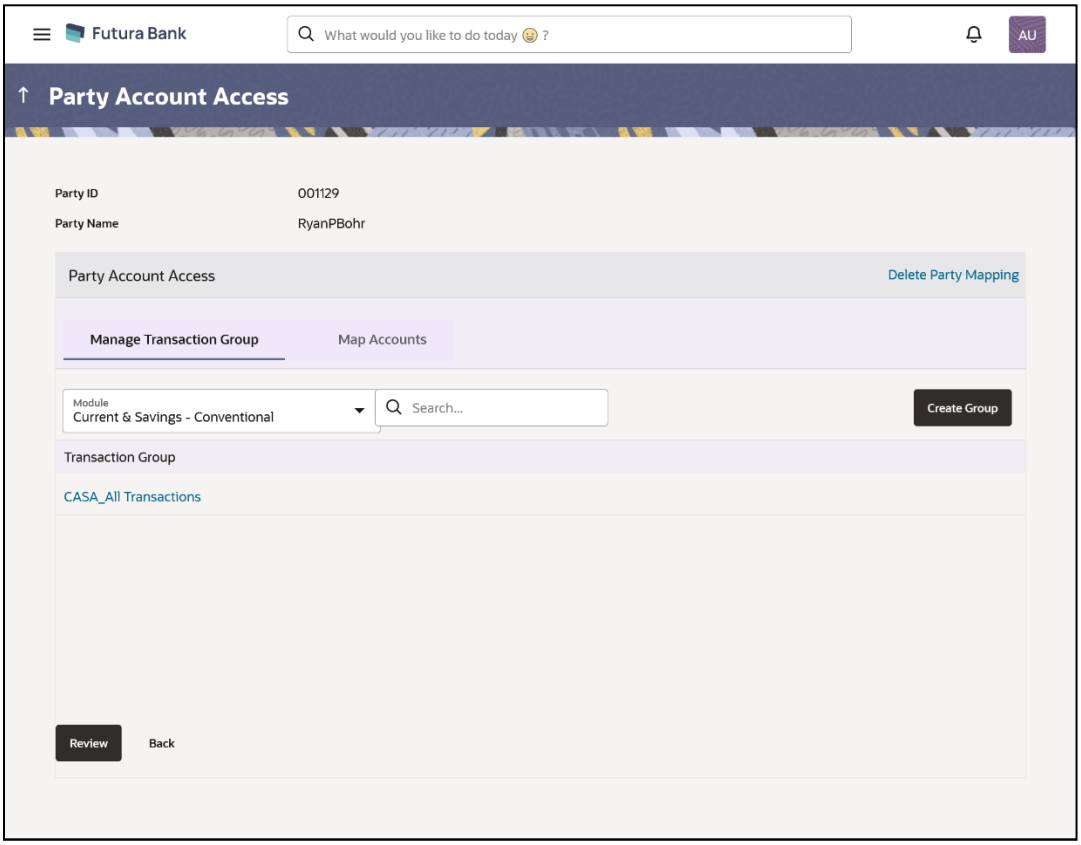
1. From the **Mapping Summary of Party** dropdown list, select the party id.
2. For a searched party, summary screen will be displayed with total accounts associated with corporate party, status of the accounts mapped for the internet banking, modified accounts if any and Auto account mapping status .
3. Click the link under the total **Mapped accounts** or **Modified accounts**, The **Party Account Access – View** (Transaction Mapping) screen appears. The search result according to the search criteria appears
   OR
   Click **Cancel** to cancel the transaction.

4. If there is no mapping done for a party, the count for the **Mapped Accounts** will be '**0'.**
5. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories.
6. Click **Map** or **Edit** (available across each banking module). The **Party Account Access - Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.

Party Account Access – Edit



Party Account Access – Edit Details



7. The Party Account Access screen has two tabs. Header of the screen shows the Party ID and Party Name. The manage Transaction Group tab lists down all the **modules, transaction groups** created.

8. Navigate and select specific **module** tab (Including viz. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts, in the first column for which account and transaction access mapping maintenance need to be setup.

9. The user can create a new **transaction group** by clicking the **'ADD'** button. On clicking **Add**, a new overlay will open where all the transactions and inquiries will be listed. User can provide a name the group and select the required transactions and inquiries and click the **save** button.
   OR
   Click **Reset** to clear added details in overlay screen.

10. A new group can also be created by **cloning/copying an existing transaction group**. Once the user selects an existing **transaction group**, system will populate the screen with the transactions selected in the copied group in editable mode. User can select or deselect some of the transactions as per requirements and create a new group by providing a different transaction group name.

11. There will be one factory shipped **Transaction group** for each module, which will have all transactions and inquiries grouped together.

Note: Factory shipped user groups cannot be deleted or modified.

12. Once the transaction groups are created, user can select specific module, along with the transaction groups and can select ‘All Accounts’ to map the selected transaction group/s to all the existing accounts under the selected party.
    OR
    If transaction groups need to be mapped to specific accounts, then the user needs to select the respective check boxes preceding the account number.
13. Once the user maps the accounts, system will show a tag as **'Modified'** followed by the transaction group name after the account number.
14. To map the new accounts, select appropriate option from **Auto Map** toggle button;
    Select **Auto** if you wish to allow access to all future Accounts across banking module.
    OR
    Select **Manual** if you wish to explicitly map new accounts and transactions.
15. User can **unmap** the transaction groups by selecting accounts and then clicking on Save button to reset their mapping with Group Corporate
16. User can click on **Delete Party Mapping** to delete all the transaction and party account access maintenance done for corporate party in one step.
17. User can drill down his search by applying Filter to search an account basis on Transaction Group, currency, mapping status
18. Click **Save** to save the maintenance, and redirect to the review page.
    OR
    Click **Back** to navigate back to previous screen..
19. The screen with success message appears. Click **OK** to complete the transaction.

10.4 Party Account Access- Delete

As part of this option, party account mapping can be deleted.

To delete account and transaction access for the party:

1. From the **Mapping Summary of Party** dropdown list, select the party id.
2. For a searched party, summary screen will be displayed with total accounts associated with corporate party, status of the accounts mapped for the internet banking, modified accounts if any and Auto account mapping status .
3. Click the link under the total **Mapped accounts** or **Modified accounts**, The **Party Account Access – View** (Transaction Mapping) screen appears. The search result according to the search criteria appears
   OR
   All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories
4. Click **Map** or **Edit** (available across each banking module). The **Party Account Access - Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
5. Click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate party in one-step.

   The application prompt the administrator with a message Are you sure you want to delete Party Account Access setup for linked Party ID – Party name with an option of Yes / No.
6. Click **Yes** to proceed with the deletion request.
   It will navigate to confirmation page with a success message and the status.
   OR
   Click **No** if you do not wish to proceed with deletion.
7. The success message and the status appear. Click **OK** to complete the transaction.
8.

FAQ

1. Is it necessary to setup Party Account Access Management before setting up User Account Access?

Yes. The party account access management setup must be done before the user level mapping of accounts and transactions.

2. What is the significance of Auto and Manual option in 'Map Accounts'?

This feature allows the administrator to configure access policies for accounts and associated transactions which may get added subsequently in the future.

Auto: Gives access to the newly added accounts and transactions of the party as soon as the account is opened. This option can be selected whenever bank administrator wishes to provide access by default

Manual: Denies the newly added accounts and transactions by default. This is to ensure that access to accounts and transactions is provided only upon receiving specific instructions from corporates

3. **Party Account Access has not been maintained for the party for Own or Linked party, still there is no 'Map' button available?**

   It is possible that the channel access and/or party preferences has not been maintained for the party whose accounts needs to be provided for access to the selected party. There will be an appropriate message provided to the user below the party details. Before proceeding with account access, administrator can visit 'Party Preferences' screen and maintain the preferences and/or channel access for the party.

4. **Will Party Account Access – Deletion for a party (Own/Linked) lead to automatic deletion of User Account Access?**

   Yes. Deletion of account access for a party will lead to automatic deletion of access for the users of that party.

5. **If I remove access of account(s) and transaction(s) for a party, will it lead to automatic access removal for the users of that party**

   Yes. Access removal at party level for an account and/or transaction will automatically remove access at user level of the selected party.

6. **I have mapped/edited/deleted party account access for a party but it is not reflecting in the system even after a successful maintenance save message?**

   There is a possibility that the maintenance is saved but the status is ‘Pending Approval’.
   For the maintenance, if there is an approval required then the changes will reflect only once the approver(s) approve the submitted request.
   If the setup does not require an approval workflow or is self / auto approved, then the same will reflect immediately.

11. User Account Access

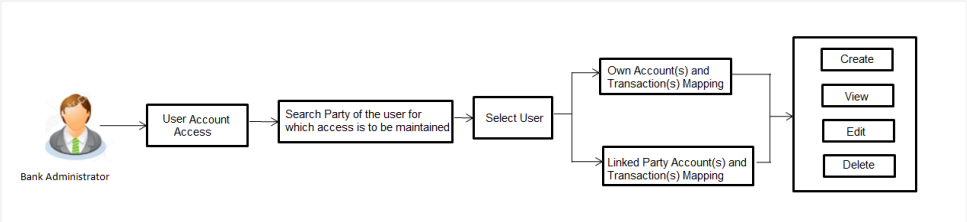
The system/Bank Administrator can set up account and transaction access for the Business Parties. Further, using this option the System/ Bank Administrator can provide access to accounts and transactions to the users mapped to the respective Business parties. If the user has access to multiple business parties, then the bank administrator can set up the Account access individually for each party and user..

Note: User Account Access is a non-mandatory step. If the Admin does not maintain the user account access for any of the Business users, system will refer to the party account access maintained for the associated party ID.

Pre-Requisites

- Account Access should be maintained for the party of the user for which access is to be maintained
- Account Access for the party should be maintained for linked party accounts if the user needs access to linked party accounts.
- Party preferences should be created for the party of the user for which access is to be maintained
- Channel Access should be enabled for party of the user for which account access is to be maintained
- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.

Workflow



Features Supported In Application

The following options are available as part of this maintenance:

- User Account Access - Mapping (Own accounts and linked party accounts)
- User Account Access – View (Own accounts and linked party accounts)
- User Account Access - Edit (Own accounts and linked party accounts)

- User Account Access - Delete (Own Accounts and linked party accounts)

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Access Management > User Account Access

11.1 User Account Access – View

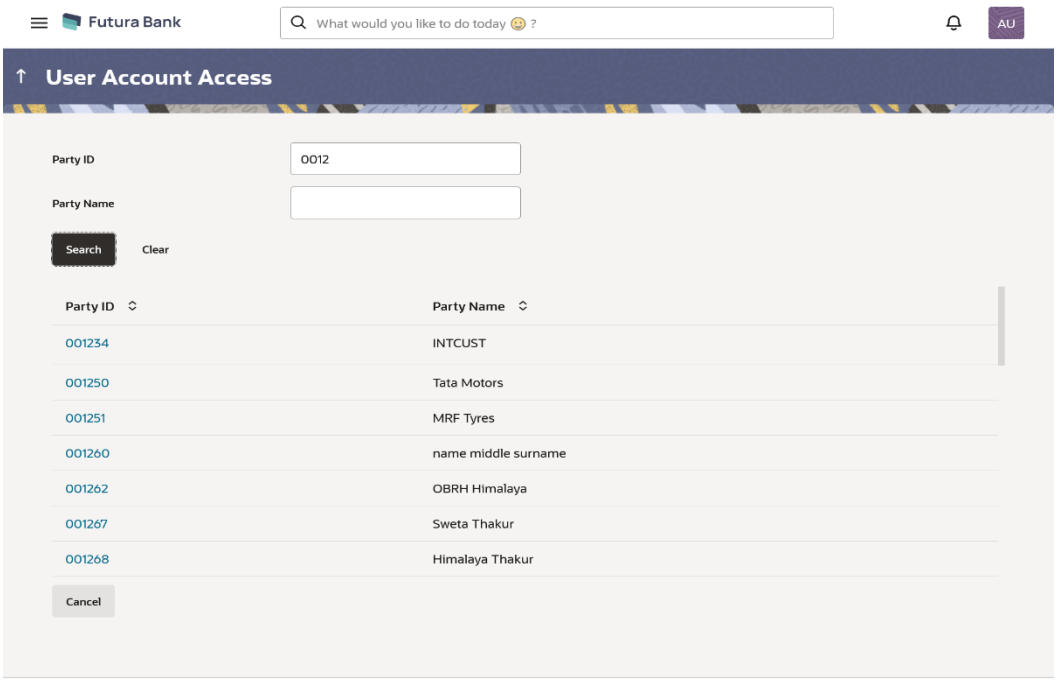
The Bank Administrator can view the list of account(s) and transactions for which access has been provided to the user.

To view the account and transaction access:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.

   Click **Search**. The system displays the result based on search criteria.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.

User Account Access - Search

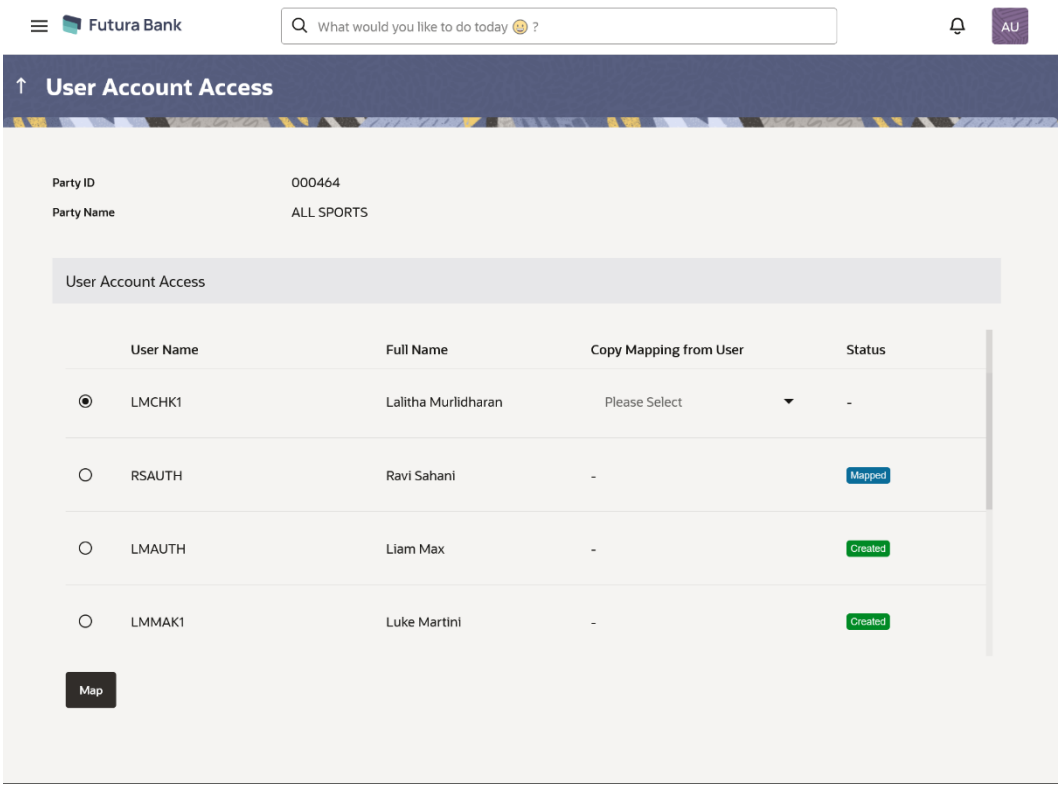


Field Description

Field Name	Description
Party ID	The party ID to be searched by the Bank Administrator.
Party Name	The name of the party.
Search Result	
Party ID	The party ID searched by the Bank Administrator.
Party Name	The name of the searched party.

1. Displays the information like user ID, contact details of the user and an indicator whether there is an account mapping done for the user.

User Account Access Details

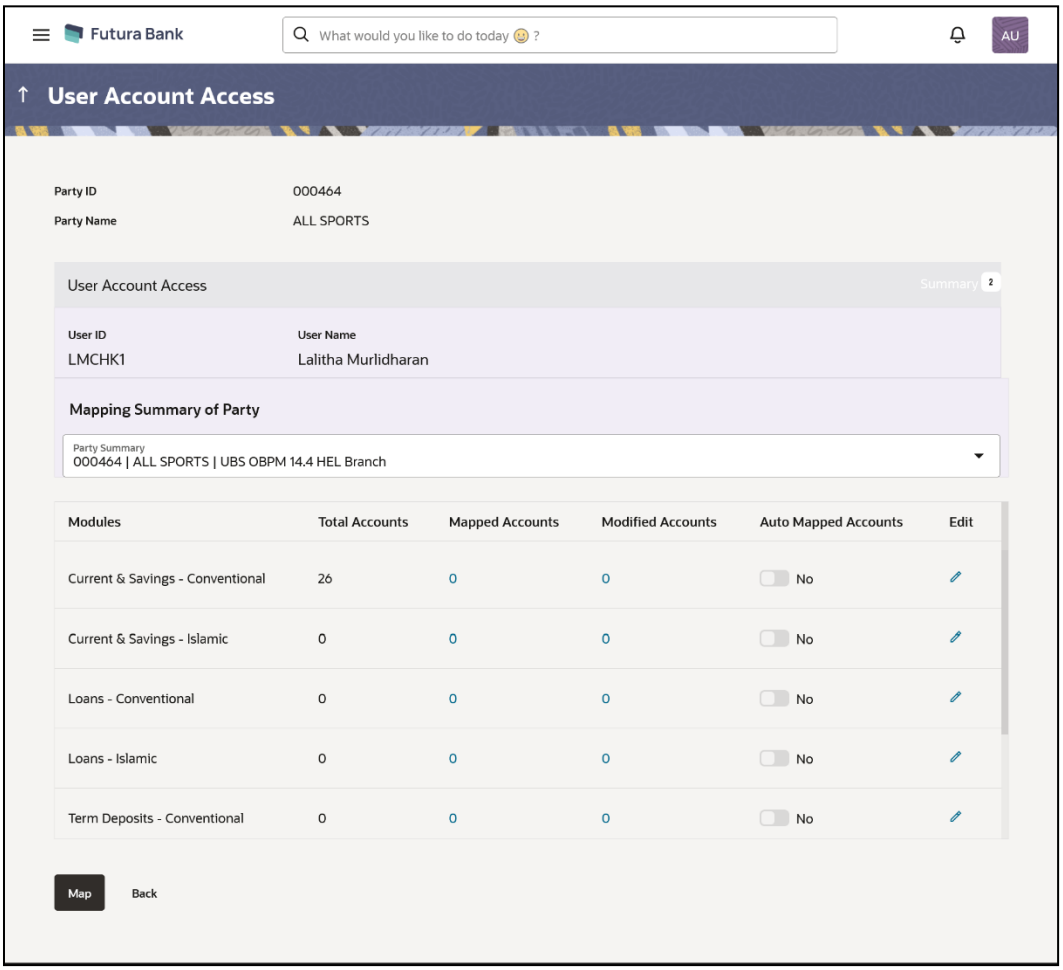


Field Description

Field Name	Description
Party ID	The party ID to be searched by the Bank Administrator.
Party Name	The name of the party.
User Account Access	
User Name	The name of the selected user.
Full Name	The full name of the selected user.
Copy Mapping from User	Select this to inherit and copy account maintenance from already setup user to a new user Note: For a user whose mapping is not done, select the user whose mapping you wish to copy from the **Copy Mapping from User** drop-down list.
Status	Displays whether mapping of the accounts is done or not. It can be: • Created • Mapped

1. For a searched user, summary screen will be displayed with total accounts associated with corporate party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .

User Account Access - Summary Results



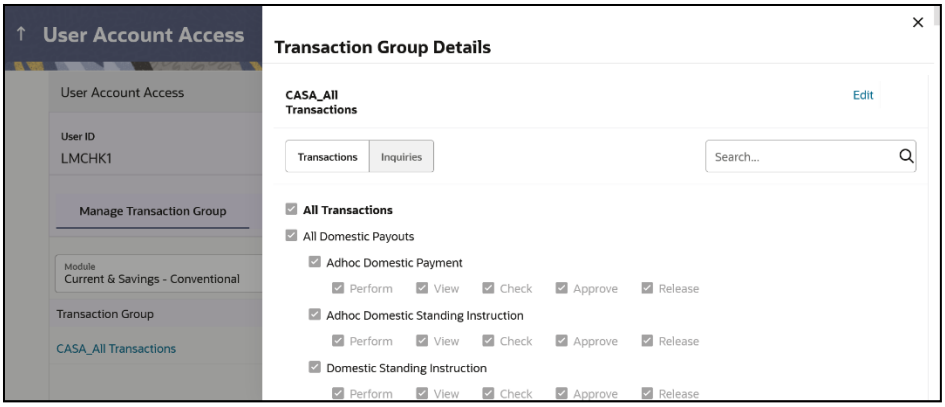
Field Description

Field Name	Description
User ID	User ID the corporate user
User Name	User name of the corporate user
Mapping Summary of Party	The corporate party for which Party accounts access is being viewed
Modules	Banking Module names
Total Accounts	Total number of accounts available under the party that can be map with corporate user.

Field Name	Description
Mapped Accounts	Number of accounts mapped to the particular account type of corporate user.
Modified Accounts	Number of accounts modified for the particular account type of corporate user.
Auto Mapped Accounts	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided
Edit or Map	Click on the icon next to every module or click on Map button to edit User account access

2. If there is no mapping done for a party, the count for the **Mapped Accounts** will be '**0'**
3. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories

User Account Access – View



Field Description:

Field Name	Description
Modules	Display name of the product for which account access is being viewed.
Mapped Transaction Group	Display the transaction groups selected to setup the user account access.
Transaction Groups Details	Display the Transaction group details with which user account access is maintained along with transaction and inquiries mapped to it.

4. The User Account Access details screen has two section. First section displays the lists down all the transaction groups mapped.
5. In the second column, user can view the **transaction group** details with all the transactions and inquiries access.
6. Click **Edit / Map** to update the **User Account Access** account mapping for new accounts and existing accounts.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.

11.2 User Account Access – Edit

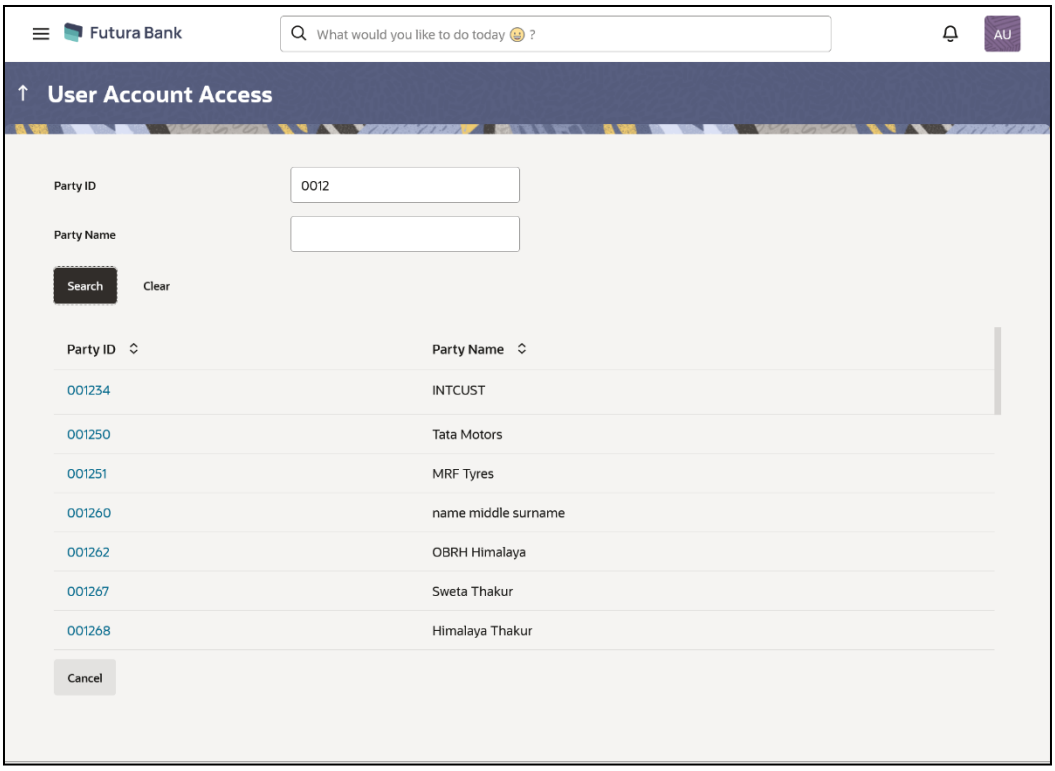
The Bank Administrator gets a request with the list of account(s) and transactions for which access details needs to be edited for a selected user of the party.

To Search and Edit the User account and transaction access:

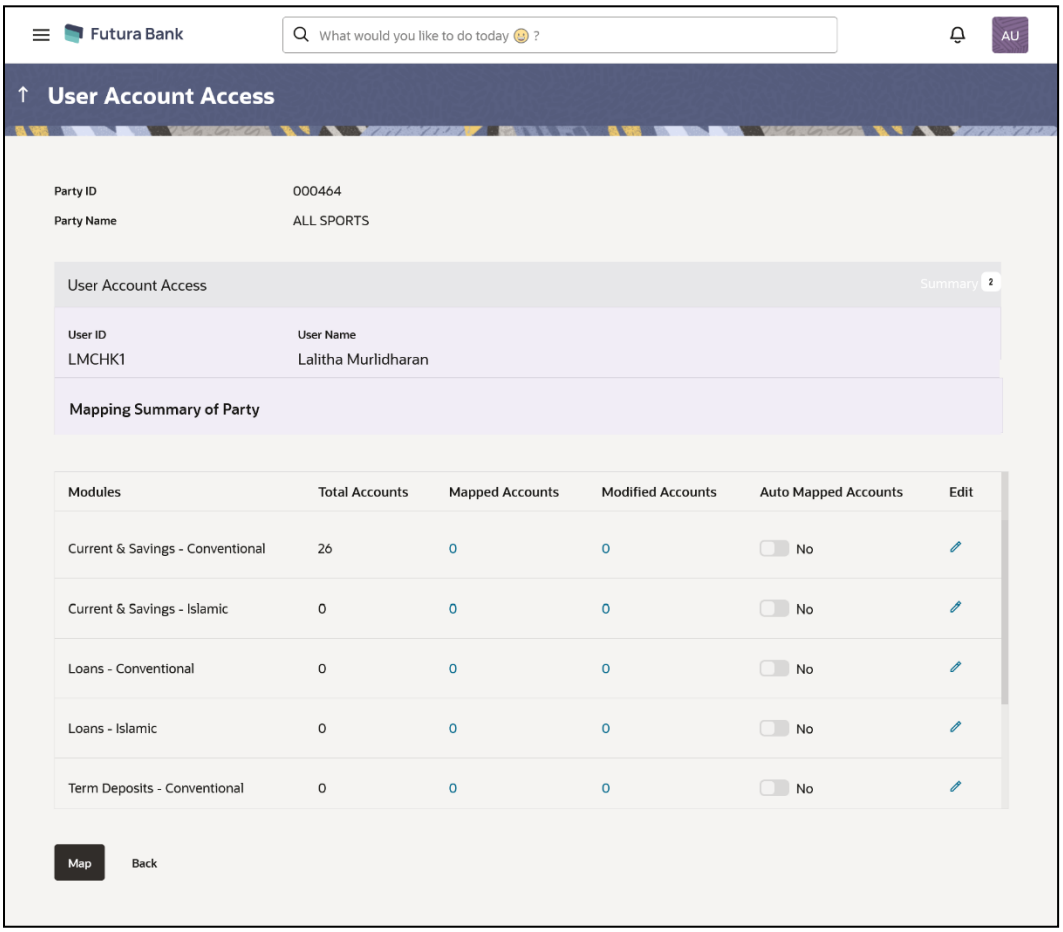
1. In the **Party ID** field, enter the party ID of the user.
   OR
   In the **Party Name** field, enter the party name of the user.

7. Click **Search**. The system displays the result based on search criteria.
   For a searched user, summary screen will be displayed with total accounts associated with corporate party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .
2. Select the user ID and click on “Map” to navigate to **Account Access summary**
3. From the **Mapping Summary of Party** dropdown list, select the corporate party id.
4. For a searched user, summary screen will be displayed with total accounts associated with corporate party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .
5. Click the link under the total **Mapped accounts** or **Modified accounts**, The **User Account Access – View** (Transaction Mapping) screen appears. . The search result according to the search criteria appears
   OR
   Click **Cancel** to cancel the transaction.
6. If there is no mapping done for a user, the count for the **Mapped Accounts** will be ‘**0’.**
7. All the accounts held by the selected user as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories
8. Click **Map** or **Edit** (available across each banking module). The **User Account Access - Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.

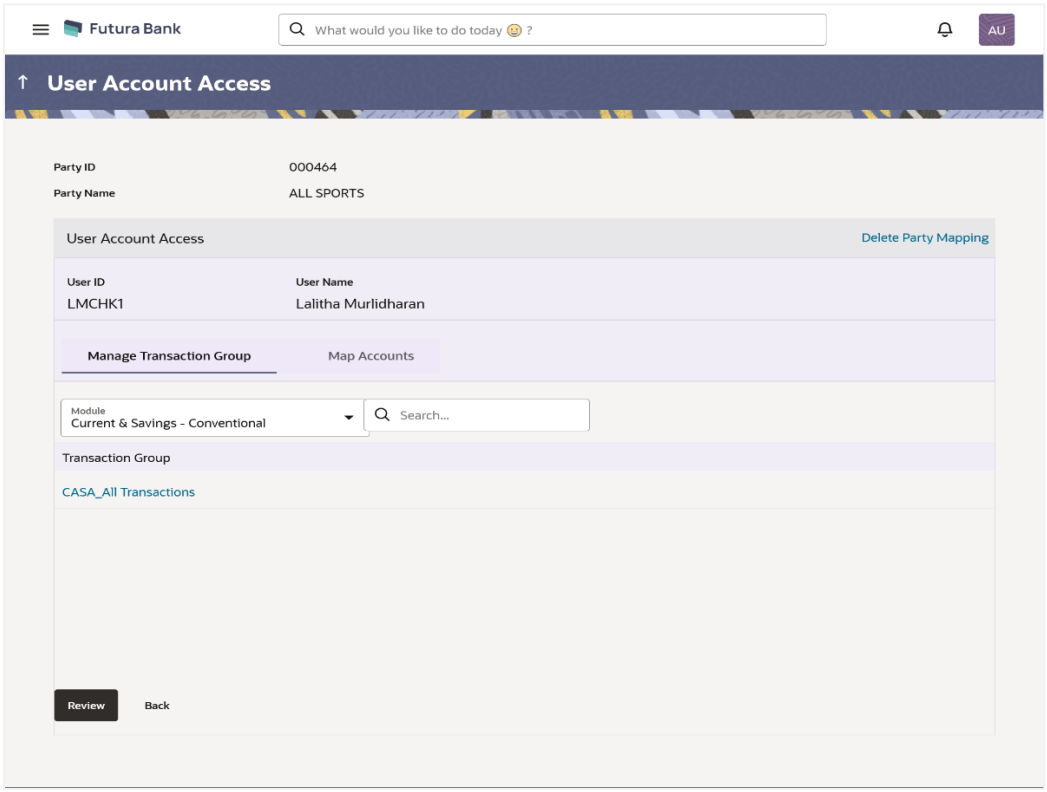
User Account Access – Search and Search Result


Futura Bank
What would you like to do today ?
AU
User Account Access
Party ID
0012
Party Name
Search
Clear
Party ID
Party Name
001234
INTCUST
001250
Tata Motors
001251
MRF Tyres
001260
name middle surname
001262
OBRH Himalaya
001267
Sweta Thakur
001268
Himalaya Thakur
Cancel

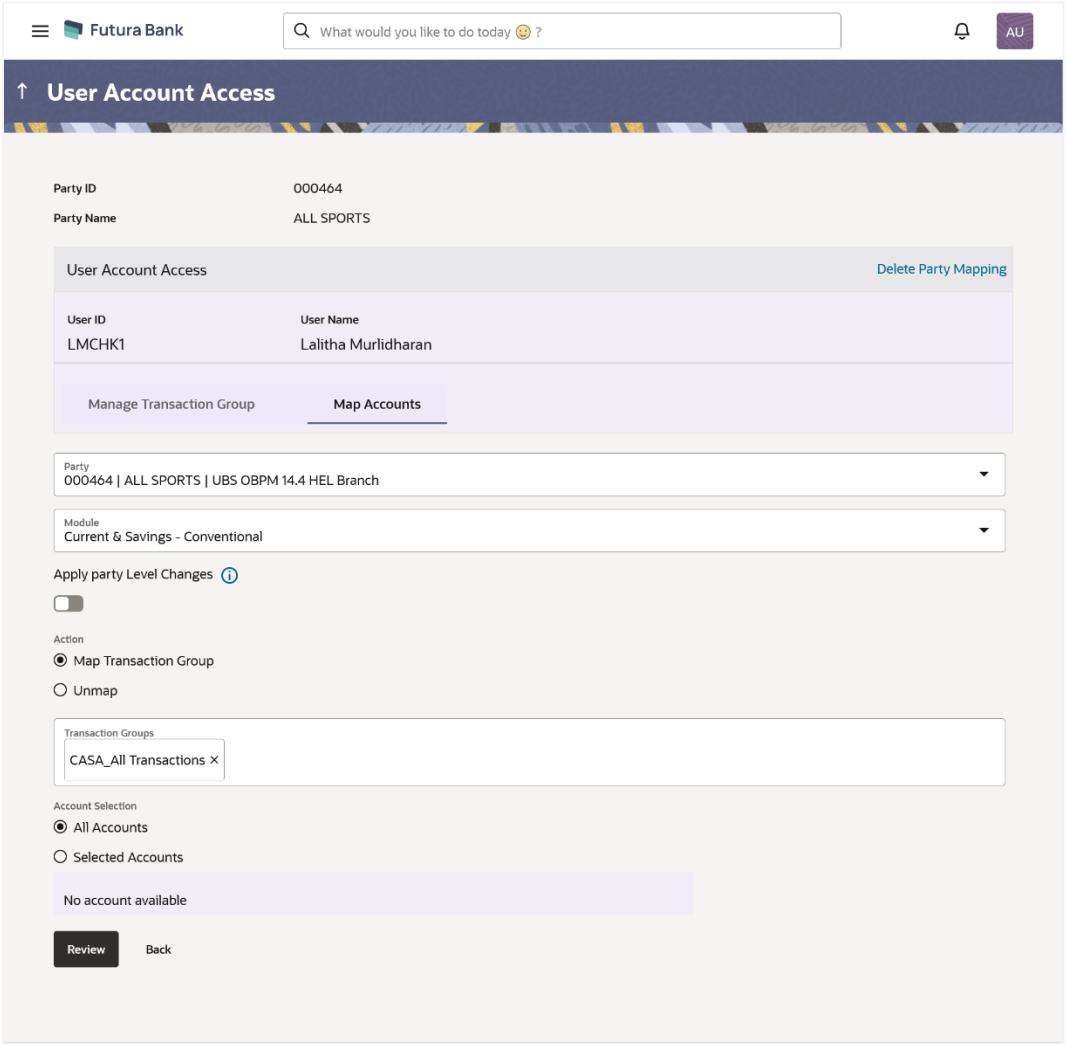
User Account Access – Summary



User Account Access – Manage Transaction Group



User Account Access – Map Accounts Tab



9. The User Account Access screen has four section. Header of the screen shows the Party ID and Party Name. First column lists down all the **modules** in tabular form, second column list down the **transaction groups** and third column list down banking module wise **account number**

10. Navigate and select specific **module** tab (Including viz. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts) In the first column for which account and transaction access mapping maintenance need to be setup.

11. In the second column, There will be one factory shipped **Transaction group** for each module, which will have all transactions and inquiries grouped together.

Note: Factory shipped user group cannot be deleted or modified.

12. Once the transaction groups are created, user can select specific module , along with the transaction groups and can select 'All Accounts' to map the selected transaction group/s to all the existing accounts under the selected party
OR

If transaction groups need to be mapped to specific accounts, then the user needs to select the respective check boxes preceding the account number.

13. Once the user maps the accounts, system will show a tag as **'Modified'** followed by the transaction group name after the account number.
14. To map the new accounts, select appropriate option from **Auto Map** toggle button;
    Select **Auto** if you wish to allow access to all future Accounts across banking module.
    OR
    Select **Manual** if you wish to explicitly map new accounts and transactions.
15. User can **unmap** the transaction groups by selecting accounts and then clicking on Save button to reset their mapping with Group Corporate
16. User can click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate user in one step.
17. User can drill down his search by applying Filter to search an account basis on Transaction Group, currency, mapping status

Note: Admin can submit the maintenance after any step. Maintenances saved so far will be sent for approval in one flow. Admin would not be able to make any changes or maintain another step for the same Group Corporate till the time the approval of the wizard is not done.

18. The **Review** screen appears. Verify the details, and click **Submit**.
    OR
    Click **Cancel** to cancel the transaction.
19. The success message of user creation appears along with the transaction reference number.

11.3 User Account Access – Create

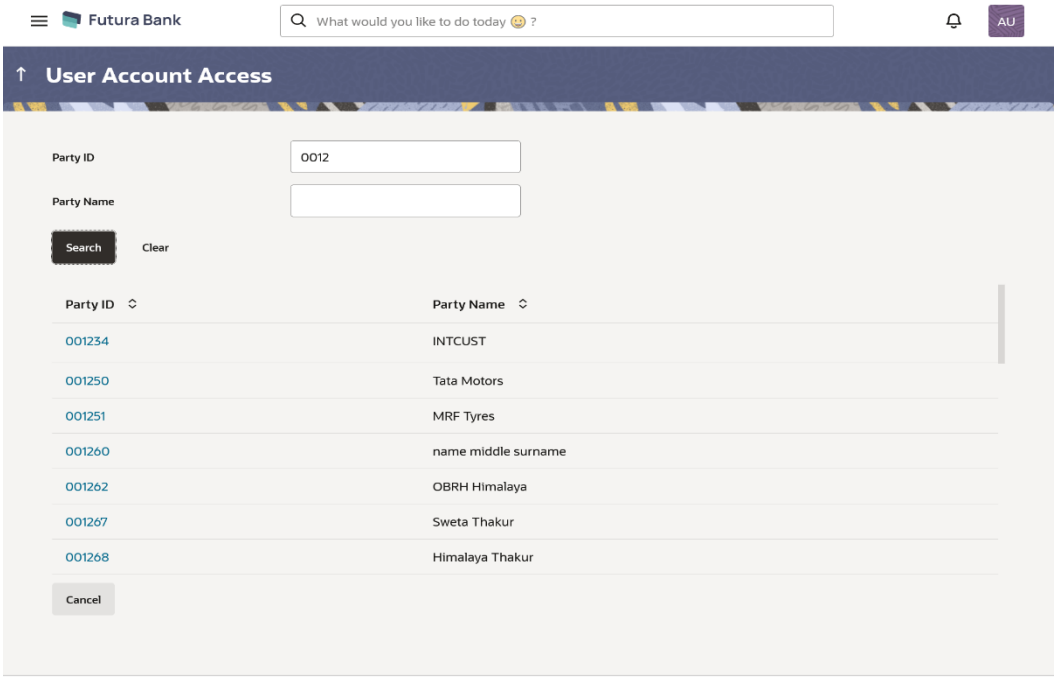
This option allows the administrator to provide account and transaction access to specific users of a party.

To provide the user with account and transaction access:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.

   Click **Search**. The system displays the result based on search criteria.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.

User Account Access - Search

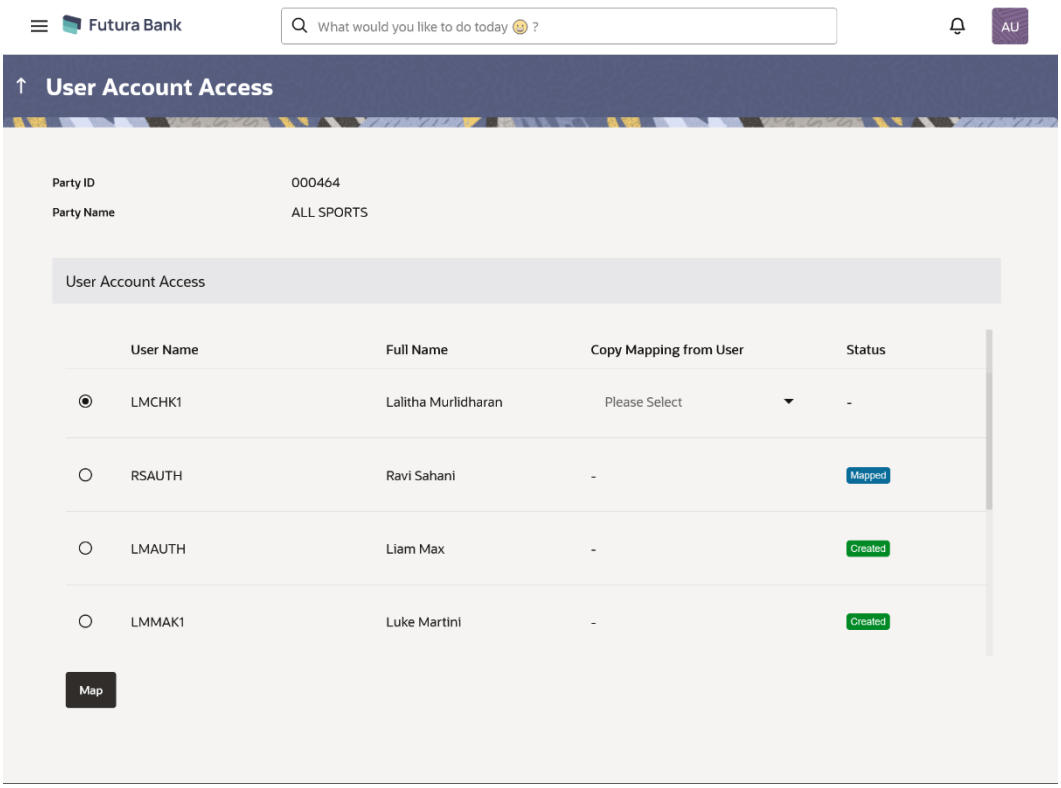


Field Description

Field Name	Description
Party ID	The party ID to be searched by the Bank Administrator.
Party Name	The name of the party.
Search Result	
Party ID	The party ID searched by the Bank Administrator.
Party Name	The name of the searched party.

2. Click on the **Party ID**. For a searched party, there will be a list of users displayed with information like username, full name of the user and an indicator whether there is an account mapping done for the user.

User Account Access Details

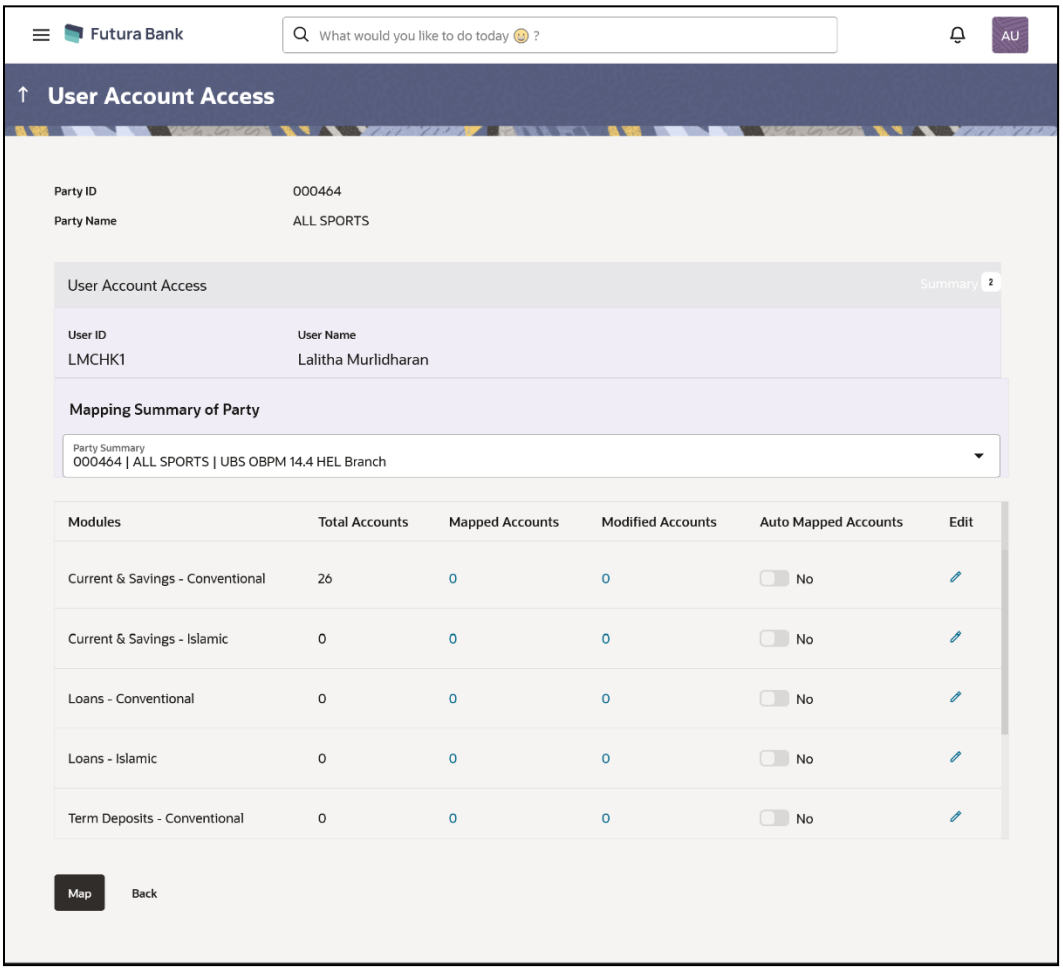


Field Description

Field Name	Description
Party ID	The party ID to be searched by the Bank Administrator.
Party Name	The name of the party.
User Account Access	
User Name	The name of the selected user.
Full Name	The full name of the selected user.
Copy Mapping from User	Select this to inherit and copy account maintenance from already setup user to a new user Note: For a user whose mapping is not done, select the user whose mapping you wish to copy from the **Copy Mapping from User** drop-down list.
Status	Displays whether mapping of the accounts is done or not. It can be: • Created • Mapped

3. Select the user ID and click on "**Map**" to navigate to **Account Access summary.**
4. For a searched user, summary screen will be displayed with total accounts associated with party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .

User Account Access – Summary



Field Description

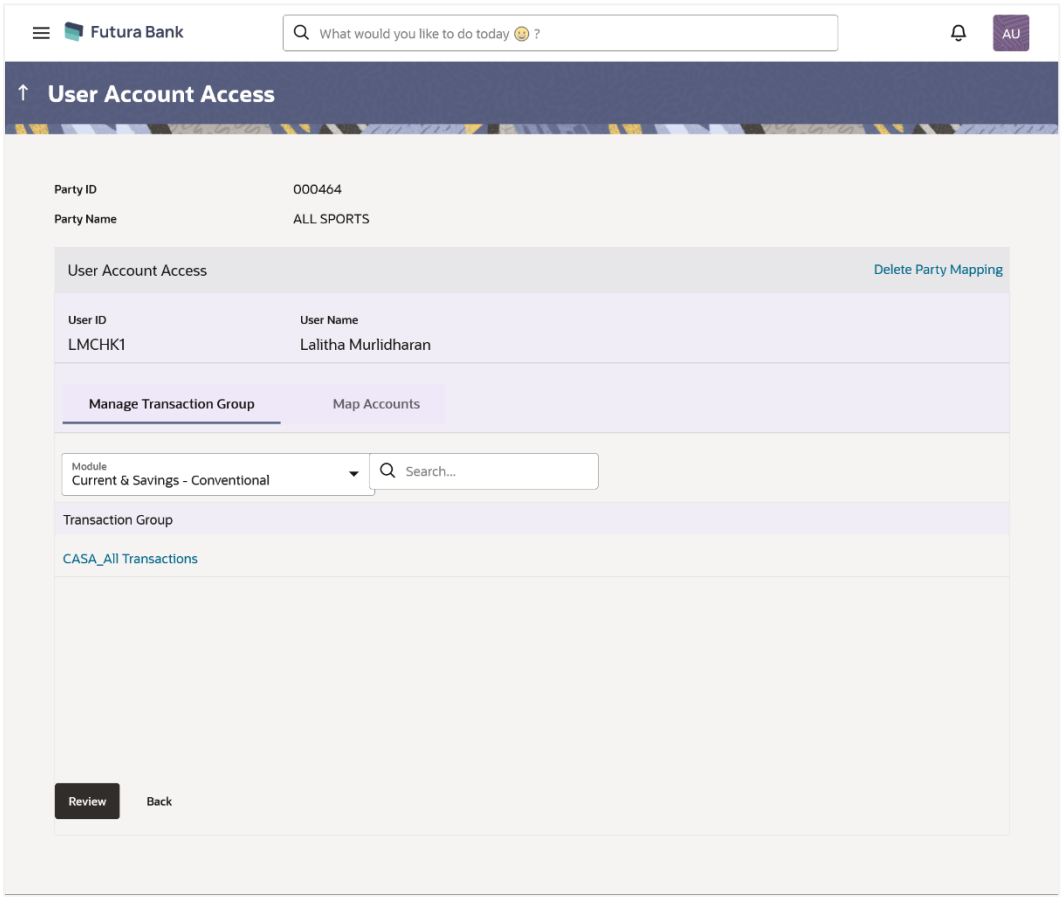
Field Name	Description
User ID	User ID the user.
User Name	User name of the user.
Mapping Summary of Party	The party for which Party accounts access is being viewed
Modules	Banking module names.
Total Accounts	Total number of accounts available under the party that can be map with user.

Field Name	Description
Mapped Accounts	Number of accounts mapped to the particular account type of user.
Modified Accounts	Number of accounts modified for the particular account type of user.
Auto Mapped Accounts	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided
Mapping Summary of Modified Transaction Group	
Modules	Banking module names.
Modified Groups	Number of transaction groups modified for the particular module.
Edit or Map	Click on the icon next to every module or click on Map button to edit User account access

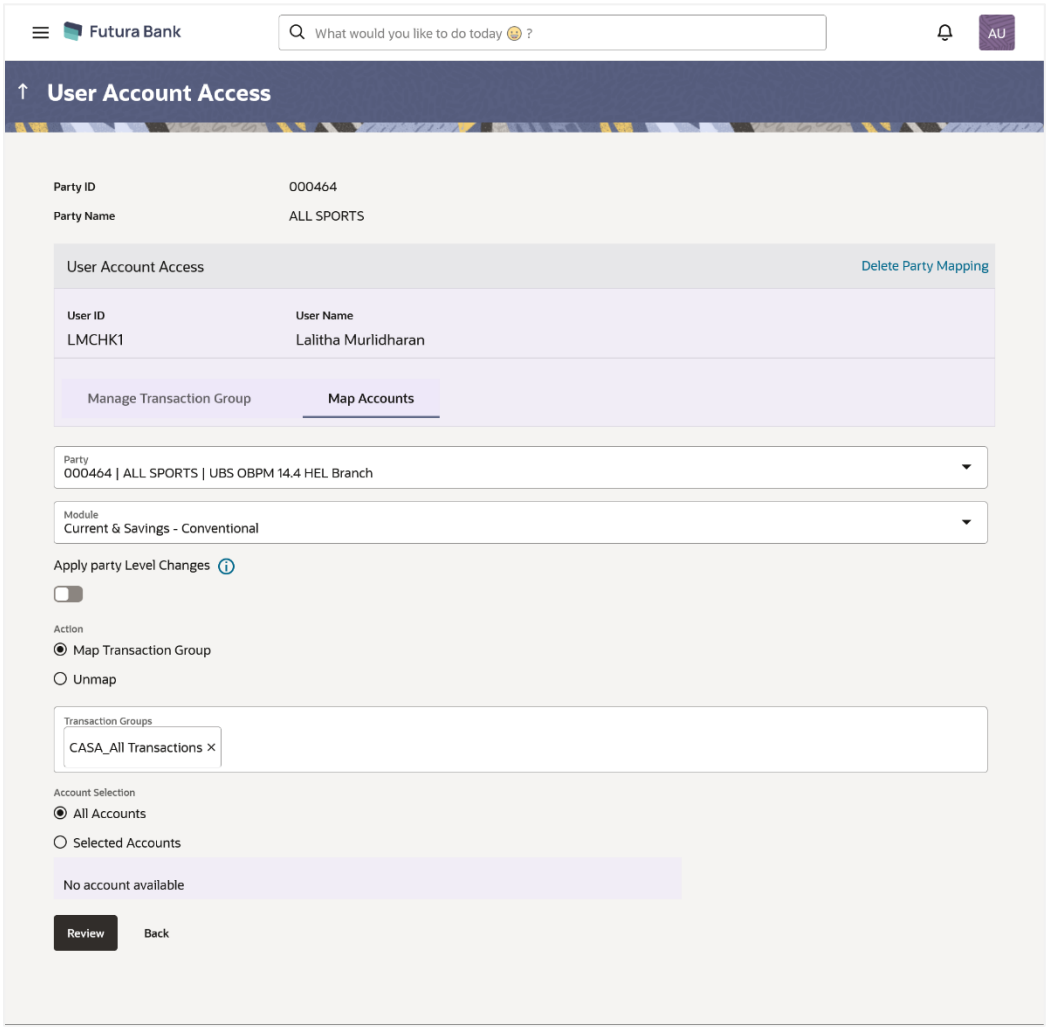
1. If there is no mapping done for a user, the count for the **Mapped Accounts** will be '**0'.**
2. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories i.e. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts.
3. User Account Access will inherit the account access setup at the party level for all the parties associated to him (party association will be done at the time of user onboarding in user management screen). The screen will show the inherited Maintenance in User Account Access screen. In the **Auto Mapped Accounts** field, toggled **ON** to allow access to all future Accounts across banking module.
   OR
   In the **Auto Mapped Accounts** field, toggled **OFF** to explicitly map new accounts and transactions manually.
4. Click on the **Modified Groups** count link to view the details of transaction groups details.

1. Click **Map** or **Edit** (available across each banking module). The **User Account Access - Create** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

User Account Access – Manage Transaction Group Tab



User Account Access – Map Accounts Tab



Field Description:

Field Name	Description
User ID	User ID the user for whom account access in being setup
User Name	User name of the user
Manage Transaction Group Tab	
Module	Select Banking Module types available under the selected party to setup account access.

Field Name	Description
Select Transaction Groups	Select the Transaction group to map transactions and maintain access in Account Access screens. Note : 1) Transaction groups mapped to the accounts at party level will be shown on this screen. 2) In user account access, the accounts can be mapped to the same transaction group to which the accounts are mapped at the party level
Transactions Groups	Search and add the transaction groups.
Map Accounts Tab	
Mapping Summary of Party	The corporate party for which user accounts access is being viewed.
Modules	Select Banking Module available under the selected party to setup account access
Apply Party level Changes	Toggle to enable to apply party level changes automatically.
Action	Option to map/unmap the transactions and maintain access in Account Access screens of Transaction Groups. The options are: • Map Transaction Group • Unmap Note: Only one transaction group can be unmapped at a time. A transaction group can be unmapped from All Accounts or Selected Accounts.
Transaction Groups	Select one or multiple Transaction group/s to map transactions and maintain access in Account Access screens. Note : 1) Transaction groups mapped to the accounts at party level will be shown on this screen. 2) In user account access, the accounts can be mapped to the same transaction group to which the accounts are mapped at the party level

Field Name	Description
Account Selection	Select accounts to map the transaction groups. The options are: • All Accounts • Selected Accounts **Note :** System will show a tag as 'Modified' followed by the transaction group name after the account number
All Accounts	Click to select all the accounts available under the selected module.
Selected Accounts	
Selected Accounts	Select the desired accounts to map the transaction group. System displays the Account Number along with the Account Name, Account Currency, and Branch Code.
Number of Accounts Selected	Number of accounts selected under the particular module.
Delete Party Mapping	Click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate users in one step.

5. In the **Manage Transaction Group** Tab;
   a. Select specific **module** tab (Including viz. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts for which account and transaction access mapping maintenance need to be setup.
   b. Click on the icon to search & select the **Transaction group/s** under selected module.

      User can modify the transaction group other than the factory shipped to select or deselect the transaction access.
   c. Click on the **Transaction Group** link the **Transaction Group Details** overlay screen appears.
      Click **Edit** to modify the transaction/ inquires.
      Click **Save** to save the changes.
6. In the **Map Accounts** Tab;
   i. From the **Module** list, select the factory shipped **Transaction group** under selected module which will have all transactions and inquiries grouped together.

Note: Factory shipped user group cannot be deleted or modified.

ii. In the **Apply Party Level Changes** field, toggle to enable to apply party level changes automatically.

iii. In **Action** field, select the desired option to map/ unmap the Transaction Group.

iv. If the **Map Transaction Group** option is selected;

v. In the **Transaction Group**s list, select the transaction Group/s to map / unmap from the drop-down list.

vi. In **Account Selection** field, select the option to map the transaction groups to all the accounts or specific accounts.

vii. Once the transaction group/s are created, user can map these transaction groups to one or multiple accounts . Click on **Map Accounts** tab and select Party, then select Transaction Groups, select the account numbers and then click on **Save** to map the transaction groups to the selected accounts.

viii. Click on the **Transaction Group link**, to view the list of transactions within the mapped transaction group in an overlay.

ix. Select **'All Accounts'** option to map/ unmap transaction groups from all accounts.
OR
If specific accounts are required to be mapped, then select the respective check boxes preceding the account number.

x. Once the user maps the accounts, system will show a tag as **'Modified'** followed by the transaction group name after the account number.

xi. To map the new accounts, select appropriate option from **Auto Map** toggle button; Select **Auto** if you wish to allow access to all future Accounts across banking module.
OR
Select **Manual** if you wish to explicitly map new accounts and transactions.

7. Once the user maps the accounts, system will show a tag as **'Modified'** followed by the transaction group name after the account number.

8. If the **Unmap** option is selected;

   i. User can **unmap** the accounts by selecting accounts and then clicking on Unmap button to reset their mapping with Group Corporate.

9. User can click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate user in one step.

10. Click on the icon to further drill down by applying new sear criteria in **Filter** overlay screen on basis of Account Number, Transaction Group, Currency, Mapping Status.

11. Click **Review** screen appears. Verify the details, and click **Submit**.
OR
Click **Back** to navigate back to previous scree.

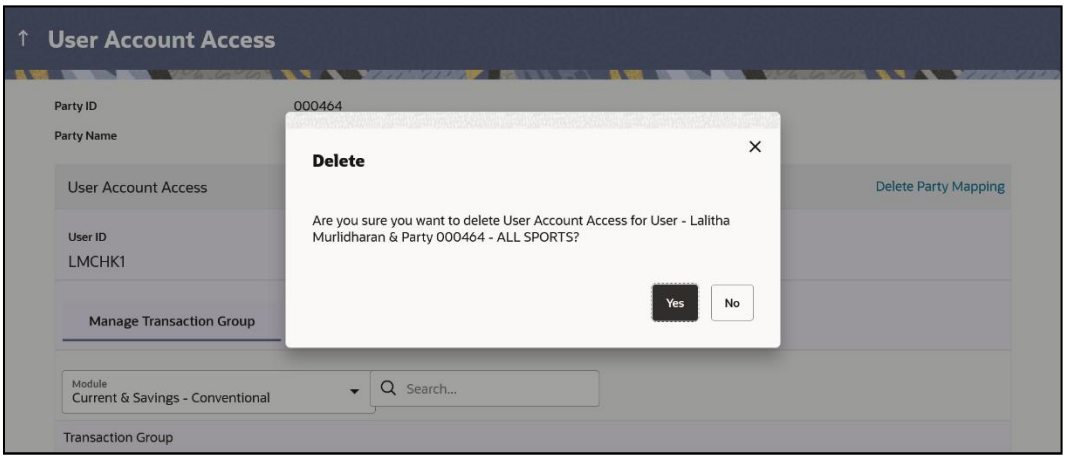
11.4 User Account Access – Delete

The Bank Administrator gets a request with the user information of a party for which access details needs to be deleted. As part of this option, account mapping can be deleted for a user.

To delete account and transaction access for the User:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**. The system displays the result based on search criteria.
   For a searched user, summary screen will be displayed with total accounts associated with corporate party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .
3. Select the user ID and click on “Map” to navigate to **Account Access summary.**
4. From the **Mapping Summary of Party** dropdown list, select the corporate party id.
5. For a searched user, summary screen will be displayed with total accounts associated with corporate party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .
6. Click the link under the total **Mapped accounts** or **Modified accounts**, The **User Account Access – View** (Transaction Mapping) screen appears. . The search result according to the search criteria appears.
   OR
   Click **Cancel** to cancel the transaction.
7. User can click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for business user in one step.

User Account Access – Delete party Mapping



   a. Click **Yes** to delete the party mapping.
      OR
      Click **No** to cancel the process.
8. **The Review** screen appears. Verify the details, and click **Submit**.
   OR
   Click **Back** to navigate back to previous screen.
9. The success message of user creation appears along with the transaction reference number.

FAQ

1. **Is it necessary to setup Party Account Access Management before setting up User Account Access?**

   Yes, party account access management setup must be done before the user level mapping of accounts and transactions.

2. **User Account Access has not been maintained for the user for Own or Linked party, still there is no 'Map' button available?**

   It is possible that the account access maintenance has not been done for the party to which the user belongs to. In such a case, bank admin will need to maintain account access for the party and only then proceed with User Account Access.

3. **Will Party Account Access – Deletion for a party (Own/Linked) lead to automatic deletion of User Account Access?**

   Yes, deletion of account access for a party will lead to automatic deletion of access for the users of that party.

4. **If I remove access of account(s) and transaction(s) for a party, will it lead to automatic access removal for the users of that party?**

   Yes, access removal at party level for an account and/or transaction will automatically remove access at user level of the selected party.

5. **I am unable to see some of the account(s) and/or transaction(s) for mapping as part of User Account Access that were available in Party Account Access for the party of the user?**

   There is a possibility that these accounts and/or transactions have not been provided access at party level of the selected user. The accounts and transactions that are unmapped at party level will not be visible at user level of the selected party.

6. **Have mapped/edited/deleted user account access for a party but it is not reflecting in the system even after a successful maintenance save message?**

   There is a possibility that the maintenance is saved but the status is 'Pending Approval'. For the maintenance, if there is an approval required then the changes will reflect only once the approver(s) approve the submitted request. If the setup does not require an approval workflow or is self / auto approved, then the same will reflect immediately.

12. Party Resource Access

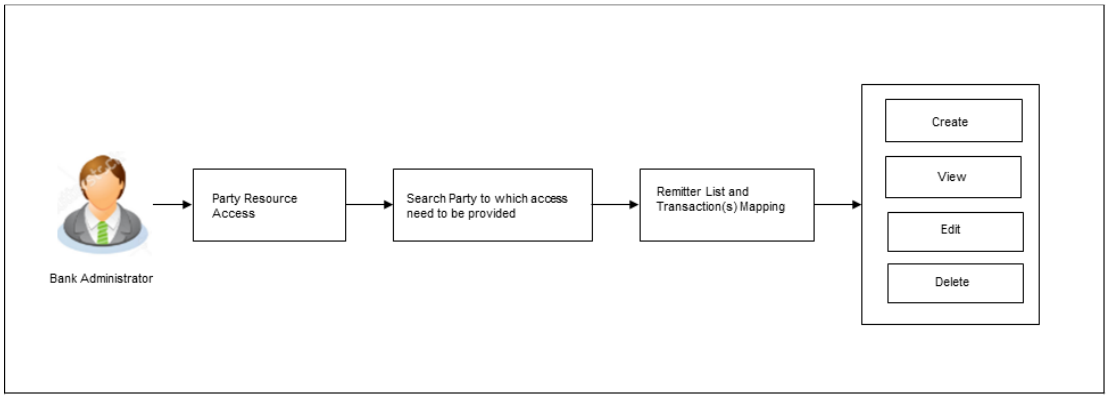
Using this maintenance, the System/ Bank Administrator can provide access to Virtual Account Management Resource 'Remitter List'. The Party Resource Access screen lists the remitter IDs for the selected Corporate.

The administrator can select a global check box of 'Map All Remitter List ' to enable all the existing remitter list under the party for channel banking. If specific remitters are required to be given access then the user needs to select the respective check boxes preceding the remitter ID.

Pre-Requisites

- Party preferences should be created for the party for which access is to be maintained
- Channel Access should be enabled for party for which resource access is to be maintained
- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.

Workflow



Features Supported In Application

The following options are available as part of this maintenance:

- Party Resource Access - Mapping
- Party Resource Access – View
- Party Resource Access - Edit
- Party Resource Access - Delete

How to reach here:

System/ Bank Administrator Dashboard > Toggle menu > Menu > Access Management > Resource Access > Party Resource Access

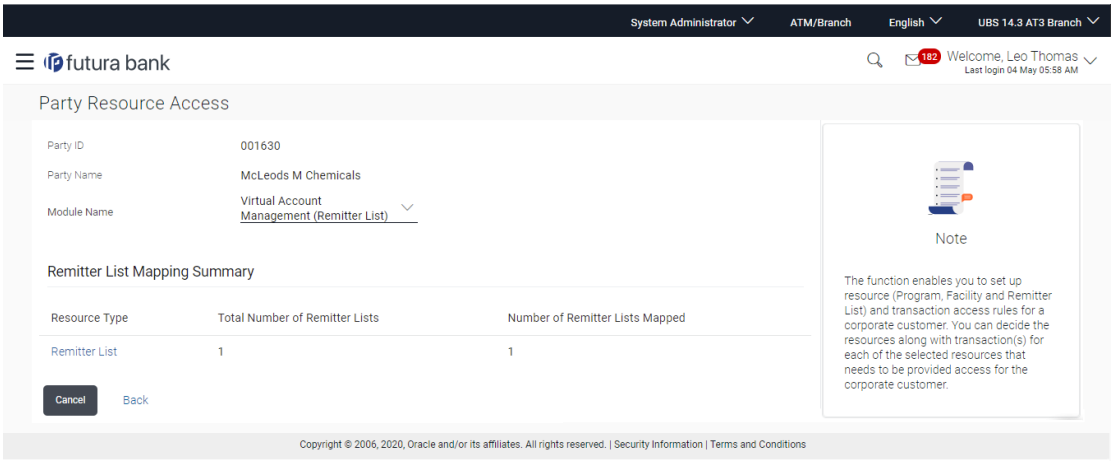
12.1 Party Resource Access - Mapping (Create)

The Bank Administrator gets a request with the Virtual Account Management Remitter list for which access needs to be provided to the party.

To provide the party with remitters access:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**. For a searched party, **Remitter List Mapping Summary** appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.

Party Resource Access - Search



Field Description

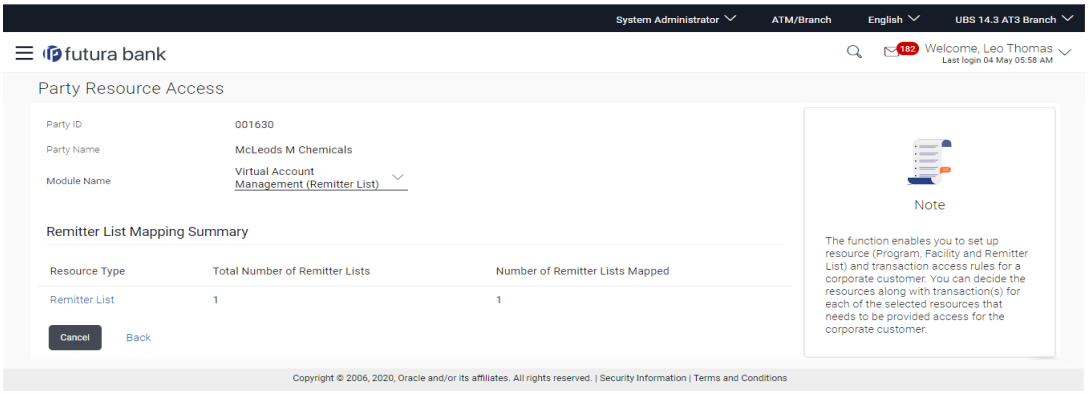
Field Name	Description
Party ID	The party id searched by the bank administrator.
Party Name	The name of the party.
Module Name	The name of the module. Only Virtual Account Management (Remitter List) is supported.

Remitter List Mapping Summary

3. If there is no mapping done for a party, there will be a message **No Remitter List mapped** with Map button.

4. Click **Map**. The **Party Resource Access - Create** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Party Resource Access - Create



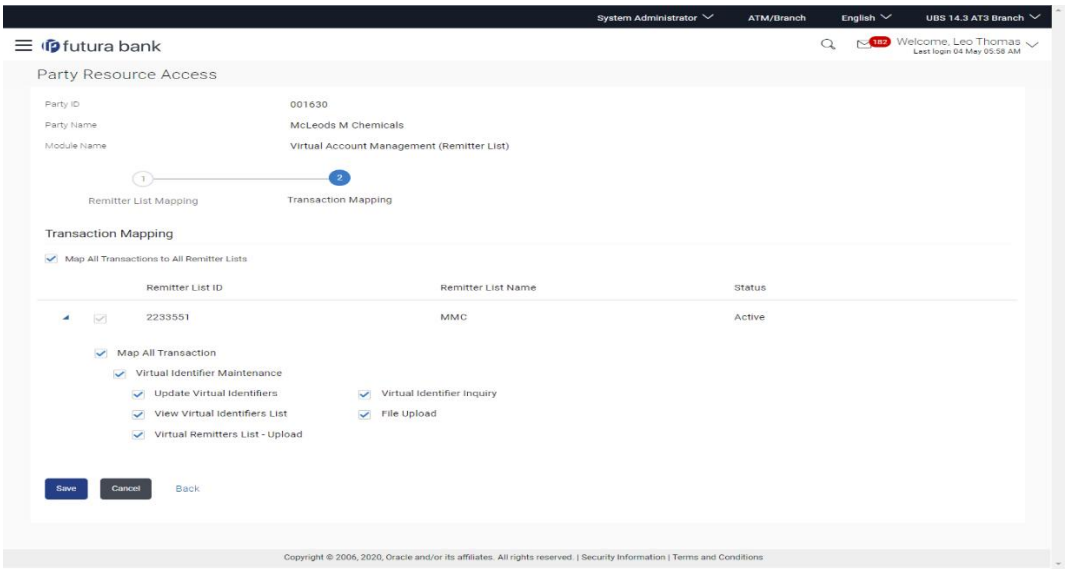
Field Description

Field Name	Description
Party ID	The party id searched by the bank administrator.
Party Name	The name of the party.
Module Name	The name of the module.
Remitter List Mapping	
Map All Remitter List	Mapping all the existing remitter list IDs to enable for channel banking.
Remitter List ID	List of remitter IDs present for the selected party.
Remitter List Name	Name of the remitter list available under the party.
Status	Status of the remitter list.

Field Name	Description
New Remitter List Mapping	Mapping of the remitters. The options can be: • Auto: gives default access to the all future newly added remitter list IDs and transactions of the party • Manual: gives specific access to future remitter list IDs. This is to explicitly map new remitter lists and transactions if access needs to be provided.

5. All the Remitter List IDs of the selected party as a relationship with the bank as available in the VAM mid-office system will be fetched and displayed.
6. Select a global check box of **Map All Remitter List** to enable all the existing remitters for channel banking (on screen, it will serve as a **Select All** function).
   OR
   If specific remitter list IDs are required to be given access then the user needs to select the respective check boxes preceding the remitter ID.
7. To map the new remitters list, select appropriate option from **New Remitter List Mapping** field;
   Select **Auto** if you wish to allow access to all future Remitter List.
   OR
   Select **Manual** if you wish to explicitly map new remitter list and transactions.
8. Click **Next**. The **Party Resource Access - Create** (Transaction Mapping) screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Party Resource Access - Transaction Mapping - Create



9. To map the transactions to the remitter ID, click ▸ against the particular remitter list ID to view the transaction mapping.
10. Select the respective check boxes preceding the transaction to be mapped.
    OR
    Select **Map All Transactions to All Remitter List**, if you want to map all the transactions to all remitter lists.
11. Click **Save** to save the changes.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.
12. The **Party Resource Access - Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.
13. The screen with success message appears along with the reference number and status of the transaction. Click **OK** to complete the transaction.

12.2 Party Resource Access- View

The Bank Administrator can view the remitter lists and transactions under each remitter list ID for which access has been provided to the party.

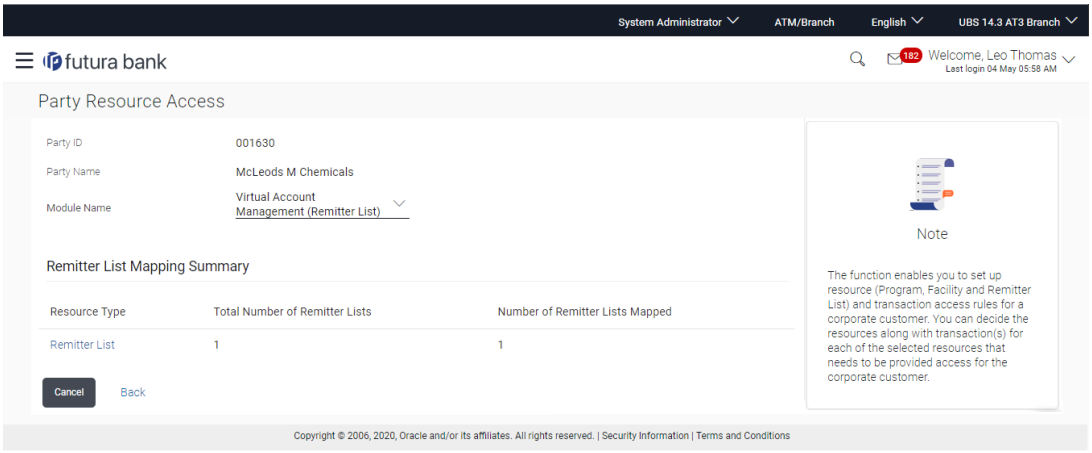
Field Description

Field Name	Description
Party ID	Party Id of the corporate user.
Party Name	Party name of the corporate user.

To view the remitter and transaction access:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**. For a searched party, **Remitter List Mapping Summary** appears that provides details of the Total no. of Remitter List IDs and the number of Remitter List IDs mapped.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.

Party Resource Access - Search Results



Field Description

Field Name	Description
Party ID	The party id searched by the bank administrator.
Party Name	The name of the party.
Module Name	The name of the module.

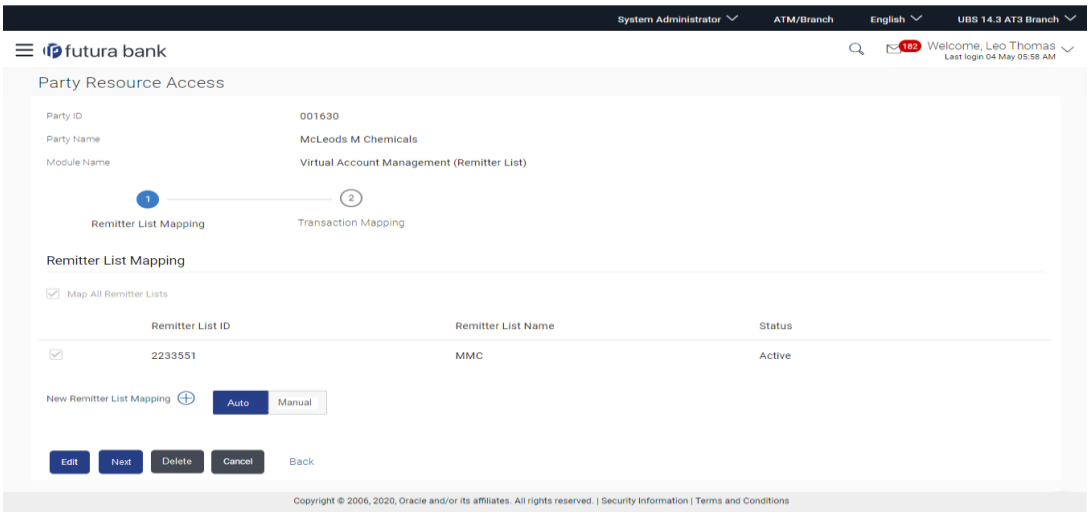
Remitter List Mapping Summary

Click on **Resource Type** to view the respective mapping details.

Resource Type	The resource types available under the party for the selected module. Resource type for Virtual Account Management module is Remitter List.
Total Number of Remitter Lists	Total number of remitter lists available under the party.
Number of Remitter Lists Mapped	Number of remitter lists mapped to the party.

3. Click the **Remitter List** link, which will navigate to the view page.
   OR
   Click **Cancel** to cancel the transaction and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.

Party Resource Access – View

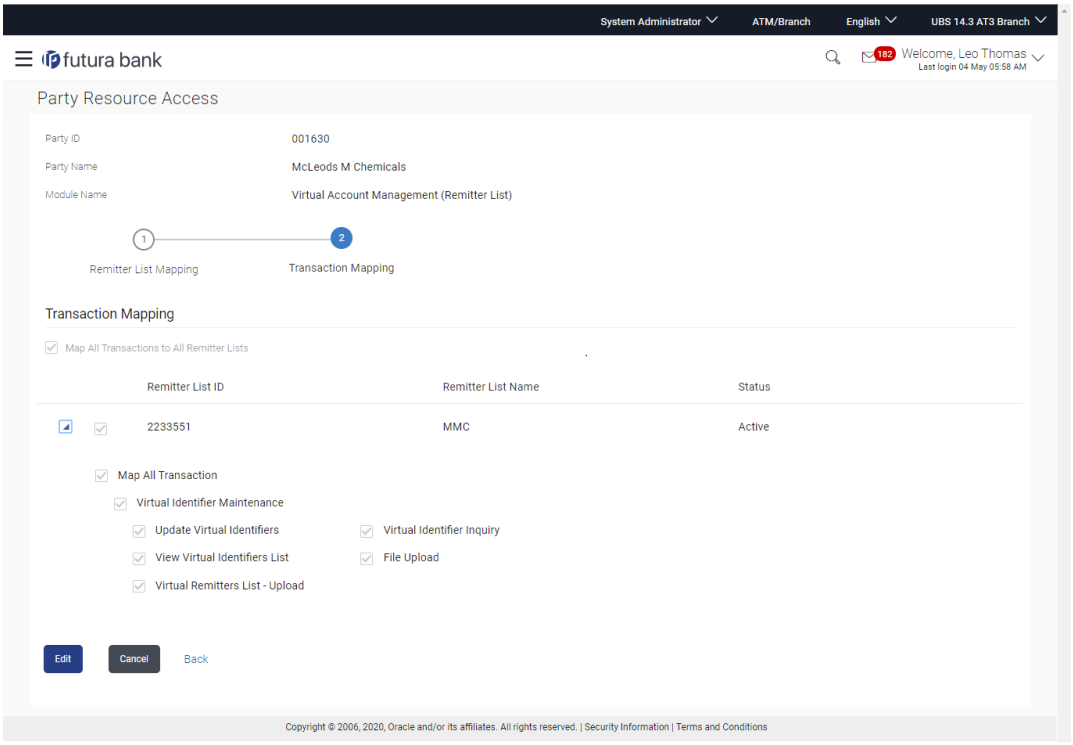


Field Description

Field Name	Description
Remitter List Mapping	
Map All Remitter List	Mapping all the remitters of the VAM module to enable for channel banking.
Remitter List ID	List of remitter IDs present in a particular resource type.
Remitter List Name	Name of the remitter list available under the party.
Status	Status of the remitter list.
New Remitter List Mapping	Mapping of the remitters. The options can be: • Auto: gives default access to the all future newly added remitter lists and transactions of the party • Manual: gives specific access to future remitter lists. This is to explicitly map new remitter lists and transactions if access needs to be provided

4. Click **Next**. The **Party Resource Access - View** screen to view the selected remitter lists and transactions enabled for the selected remitter lists appears.
   OR
   Click **Edit** to modify the remitter list mapping.
   OR
   Click **Delete** to delete the Party Resource Access setup.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Party Resource Access - Transaction Mapping- View



5. Click ▸ against the particular Remitter List to view the mapped transactions.
   OR
   Click **Edit** to update transaction mapping.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

12.3 Party Resource Access - Edit

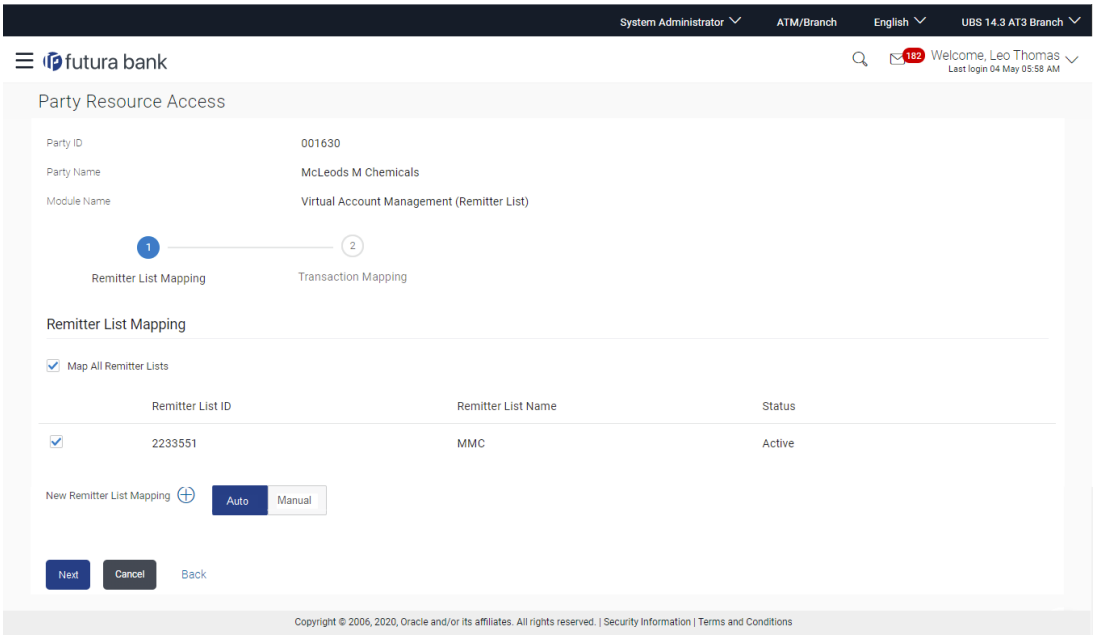
The Bank Administrator gets a request with the list of remitter lists and transactions under each Remitter List for which access details needs to be edited for the party.

To edit remitter lists and transaction access for the party:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**. For a searched party, **Remitter List Mapping Summary** appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.
3. If there is no mapping done for a party , the message **No Resource mapped for the party** with **Map** option appears.

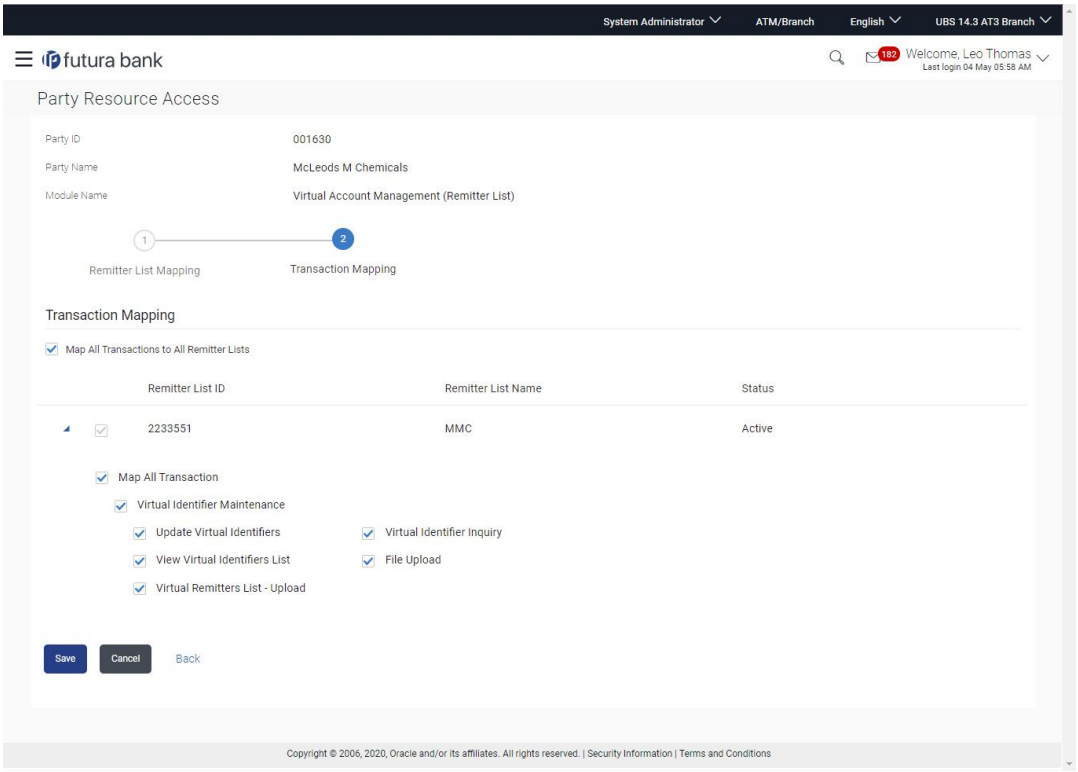
4. Click the **Remitter Type** link to view/edit the details. The **Party Resource Access**- View screen appears.
5. Click **Edit**. The **Party Resource Access - Edit** screen appears.
   This enables the selection and de-selection option against the Remitter List IDs and allows changing the map remitters from Auto to Manual and vice-versa.
   OR
   Click **Next** to go to the next tab (Transaction Mapping).
   OR
   Click **Delete** to delete the Party Resource Access setup.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Party Resource Access - Remitter List Mapping - Edit



6. To map the new resources (remitter lists), select appropriate option from **New Remitter List Mapping** field;
   Select **Auto** if you wish to allow access to all future remitter list.
   OR
   Select **Manual** if you wish to allow specific access to all future remitter list.
7. Select the respective check boxes preceding the **Remitter List ID** to be mapped.
   OR
   Select **Map All Remitter List**, if you want to map all the remitters.
8. Click **Next**. The **Party Resource Access - Edit** screen with mapped transaction - to the remitter appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Party Resource Access - Transaction Mapping - Edit



9. To map the transactions to the Remitter lists, click ▶ against the particular remitter list ID to view the transaction mapping.
10. Select the respective check boxes preceding the transaction to be mapped.
    OR
    Select **Map All Transactions**, if you want to map all the transactions to all remitter list IDs.
11. Click **Save** to save the changes.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.
12. The **Party Resource Access - Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.
13. The screen with success message appears along with the reference number and status of the transaction. Click **OK** to complete the transaction.

12.4 Party Resource Access - Delete

As part of this option, remitter list mapping and /transaction mapping can be deleted.

To delete remitter list and transaction access for the party:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**. For a searched party, **Remitter List Mapping Summary** section appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.
3. If there is no mapping done for a party (own/ linked), the message **No Remitters mapped for the party** with **Map option** appears.
4. Click the **Remitter List** link to view/delete the details. The **Party Resource Access** - View screen appears.
5. Click **Delete**. The application prompt the administrator with a message 'Are you sure you want to delete Remitter List Mapping setup for Party ID – Party name' with an option of Yes / No.
6. Click **Yes** to proceed with the deletion request.
   It will navigate to confirmation page with a success message and the status.
   OR
   Click **No** if you do not wish to proceed with deletion.
7. The success message and the status appears.
   Click **OK** to complete the transaction.

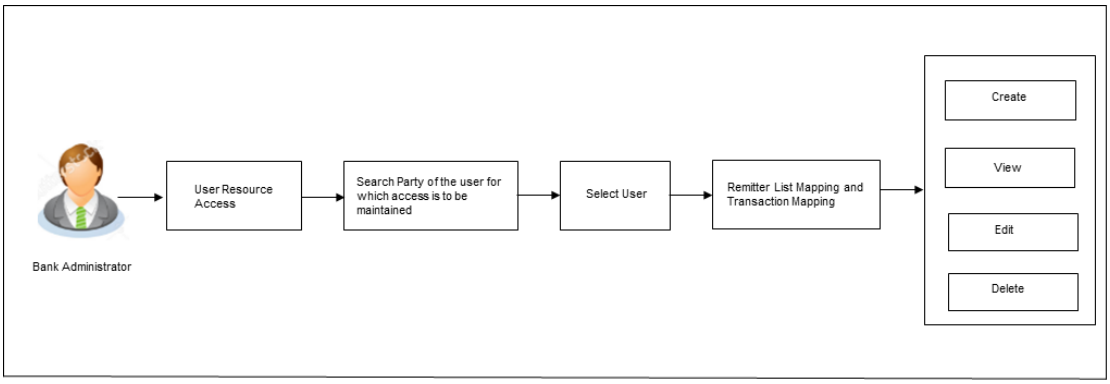
13. User Resource Access

Using this option the System/ Bank Administrator can set up remitter list mapping and transaction access for user(s) of the corporate party. This maintenance can be done only after the Party Resource Access is setup for the party of the user(s).

Pre-Requisites

- Resource Access should be maintained for the party of the user for which access is to be maintained
- Party preferences should be created for the party of the user for which access is to be maintained
- Channel Access should be enabled for party of the user for which resource access is to be maintained
- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.

Workflow



Features Supported In Application

The following options are available as part of this maintenance:

- User Resource Access - Mapping
- User Resource Access – View
- User Resource Access - Edit
- User Resource Access - Delete

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > *Menu* > *Access Management* > Resource Access > User Resource Access

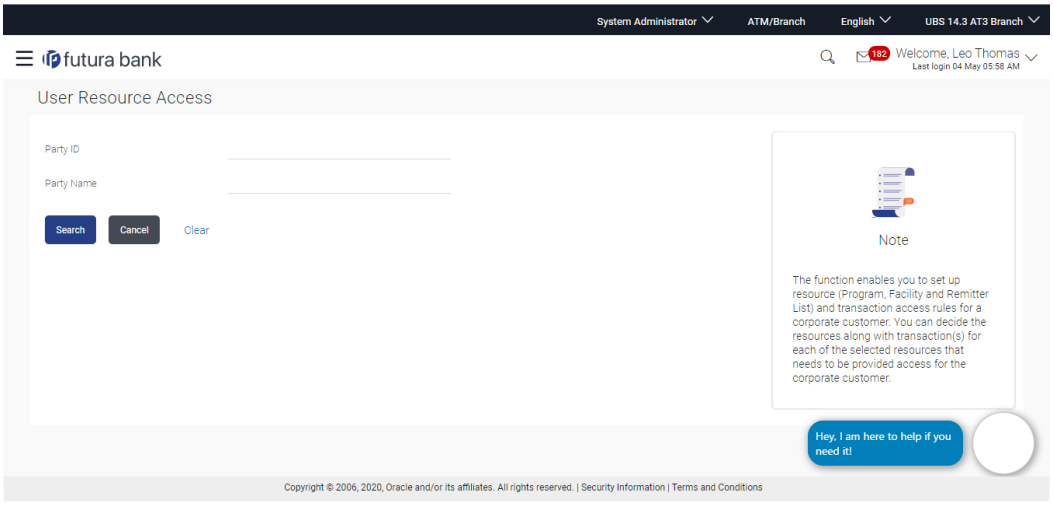
13.1 User Resource Access - Mapping (Create)

This option allows the administrator to provide access to specific users of a party.

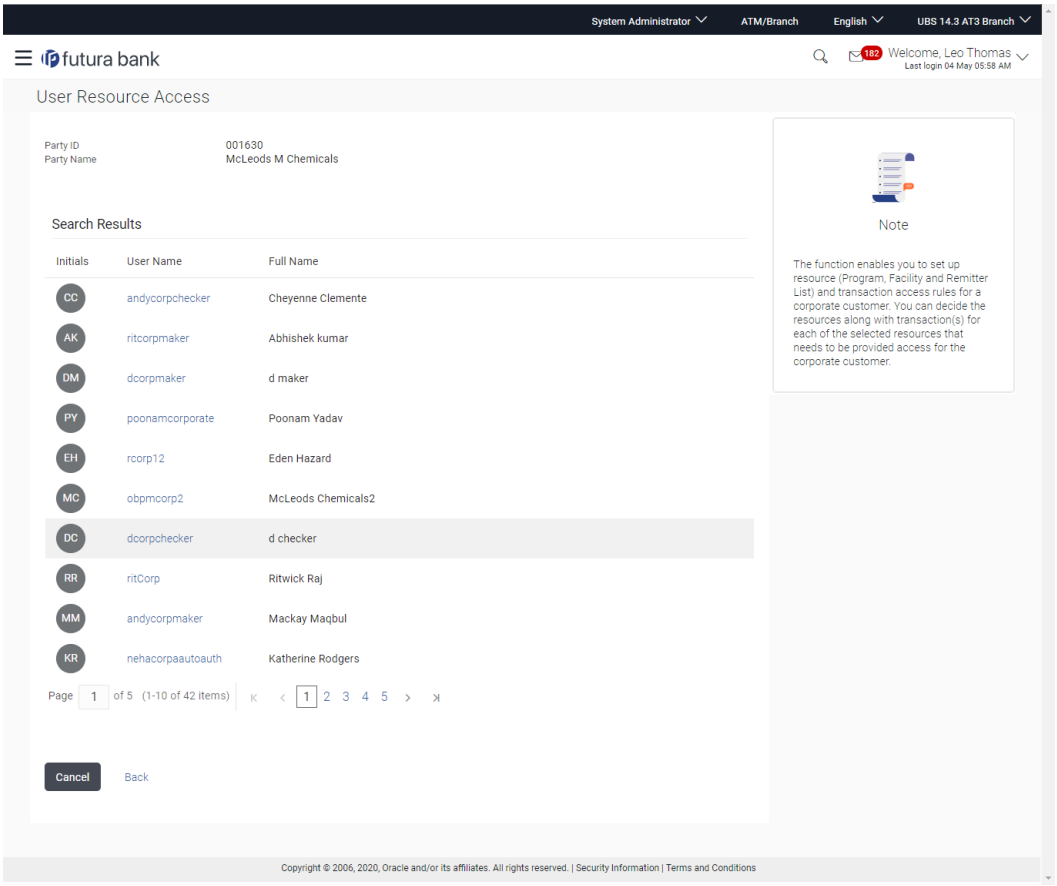
To provide the user with account and transaction access:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**.
   For a searched party, there will be a list of users displayed with information like user ID, full name of the user and initials of the user.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.

User Resource Access – Search



User Resource Access - Search Result

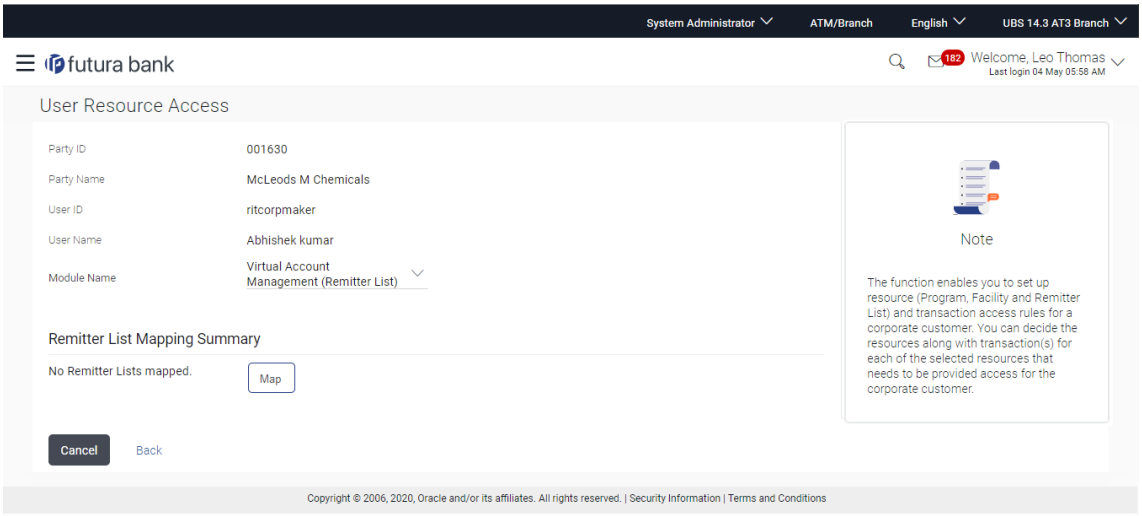


Field Description

Field Name	Description
Party ID	The party ID searched by the Bank Administrator.
Party Name	The name of the party.
Search Result	
Initials	Initials of the user.
User Name	User name of the user
Full Name	Full name of the user.

3. Click the **User Name** link against the user record for which you want to create the mapping.
   The **User Resource Access – Mapping Summary** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
4. If there is no mapping done for the user for a party, there will be a message **No Remitter List mapped** with **Map** button.
5. If the access for the party to which the user belongs to is not done, then there will be no Map button.

User Resource Access – Summary Page



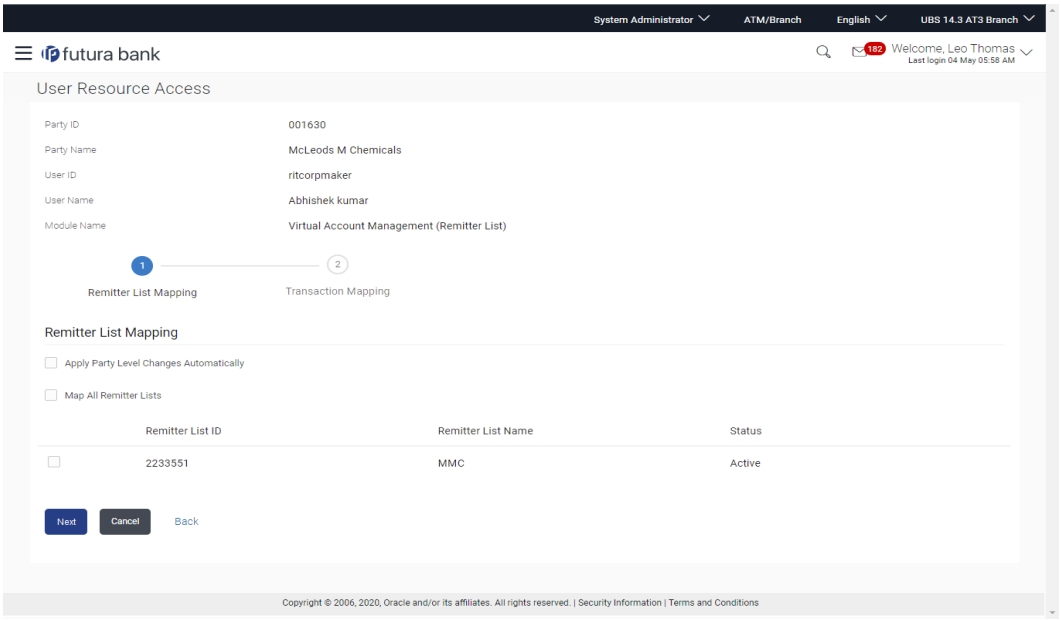
Field Description

Field Name	Description
Party ID	The party ID searched by the Bank Administrator.
Party Name	The name of the party.
User ID	User ID of the selected user.
User Name	User name of the selected user
Module Name	The name of the module. Only Virtual Account Management (Remitter List) is available.

Remitter List Mapping Summary

6. Click **Map**. The **User Resource Access - Create** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

User Resource Access - Create



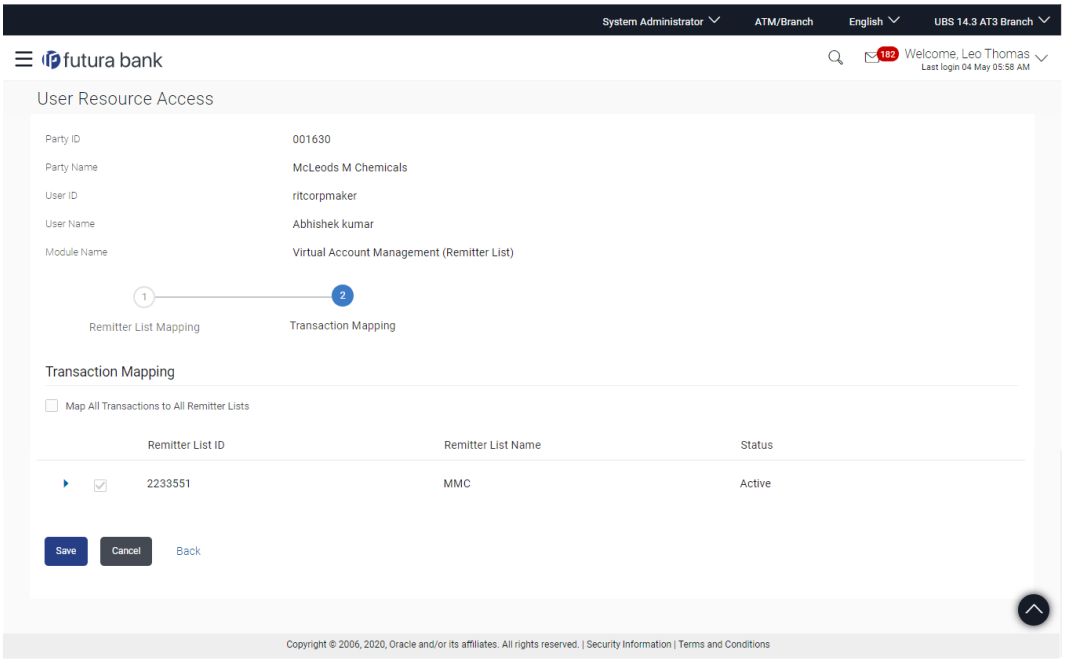
Field Description

Field Name	Description
Party ID	The party ID searched by the Bank Administrator.
Party Name	The name of the party.
User ID	User ID of the selected user.
User Name	User name of the selected user
Module Name	The name of the module.
Remitter List Mapping	
Apply Party Level Changes Automatically	User will get access to remitters that are allowed/ disallowed at the party level.

Field Name	Description
Map All Remitter List	Mapping all the remitters of the VAM module to the existing resource.
Remitter List ID	List of remitter IDs present in a particular resource type.
Remitter List Name	Name of the remitter list available under the party.
Status	Status of the remitter access for the party

7. All the remitters held by the selected party as a relationship with the bank as available in the core banking system will be fetched and displayed.
8. Select a global check box of **Map All Remitter List** to enable all the existing remitters for channel banking (on screen, it will serve as a **Select All** function).
   OR
   If specific remitter is required to be given access to the user, then the bank administrator needs to select the respective check boxes preceding the remitter ID.
9. Select **Apply Party Level Changes Automatically** to automatically apply the party changes.
10. Click **Next**. The **User Resource Access - Create** (Transaction Mapping) screen appears.
    OR
    Click **Back** to navigate to the previous screen.
    OR
    Click **Cancel** to cancel the transaction.

User Resource Access - Transaction Mapping - Create

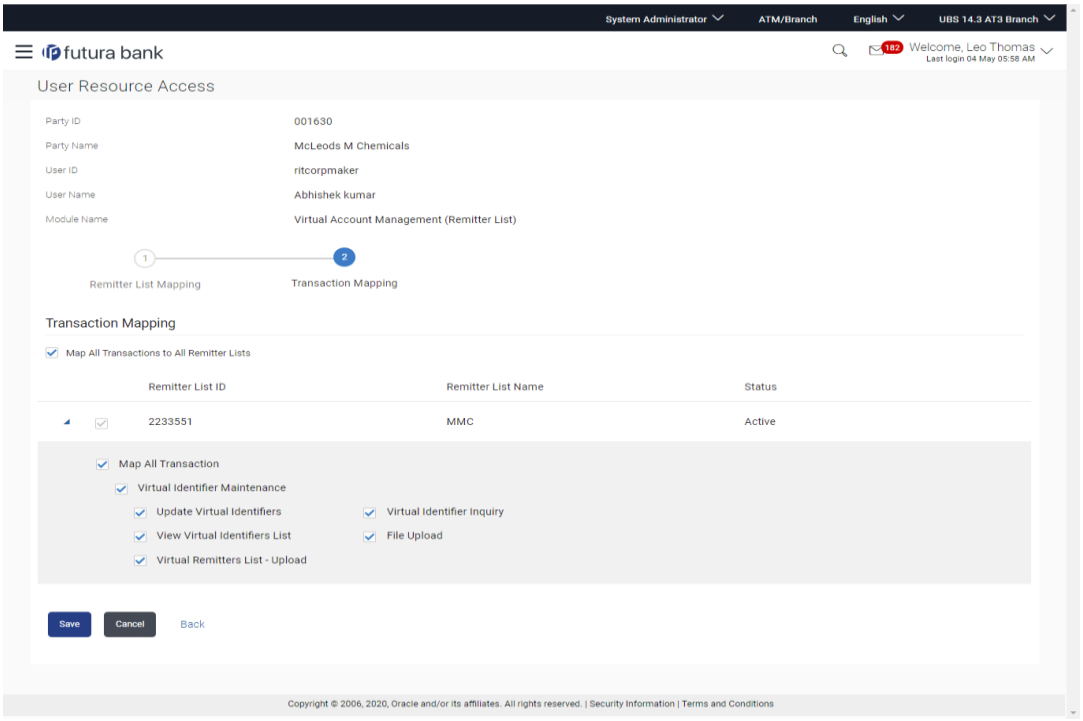


Field Description

Field Name	Description
Party ID	The party ID searched by the Bank Administrator.
Party Name	The name of the party.
User ID	User ID of the selected user.
User Name	User name of the selected user
Module Name	The name of the module.
Transaction Mapping	
Map All Transactions to All Remitter List	Mapping all the transactions to all the remitter list.
Remitter List ID	List of remitter IDs present in a particular resource type.
Remitter List Name	Name of the remitter list available under the party.
Status	Status of the remitter access for the party

11. To map the transactions to the account, click ▸ against the particular remitter ID to view the transaction mapping.

User Resource Access - Transaction Mapping (Map Transaction) - Create



12. Select the respective check boxes preceding the transaction to be mapped.
    OR
    Select **Map All Transactions**, if you want to map all the transactions to all accounts.
13. Select **Apply Party Level Changes Automatically** to automatically apply the party changes.
14. Click **Save**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.
15. The **User Resource Access - Review** screen appears. Verify the details, and click Confirm.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.
16. The screen with success message appears along with the reference number and status of the transaction. Click **OK** to complete the transaction.

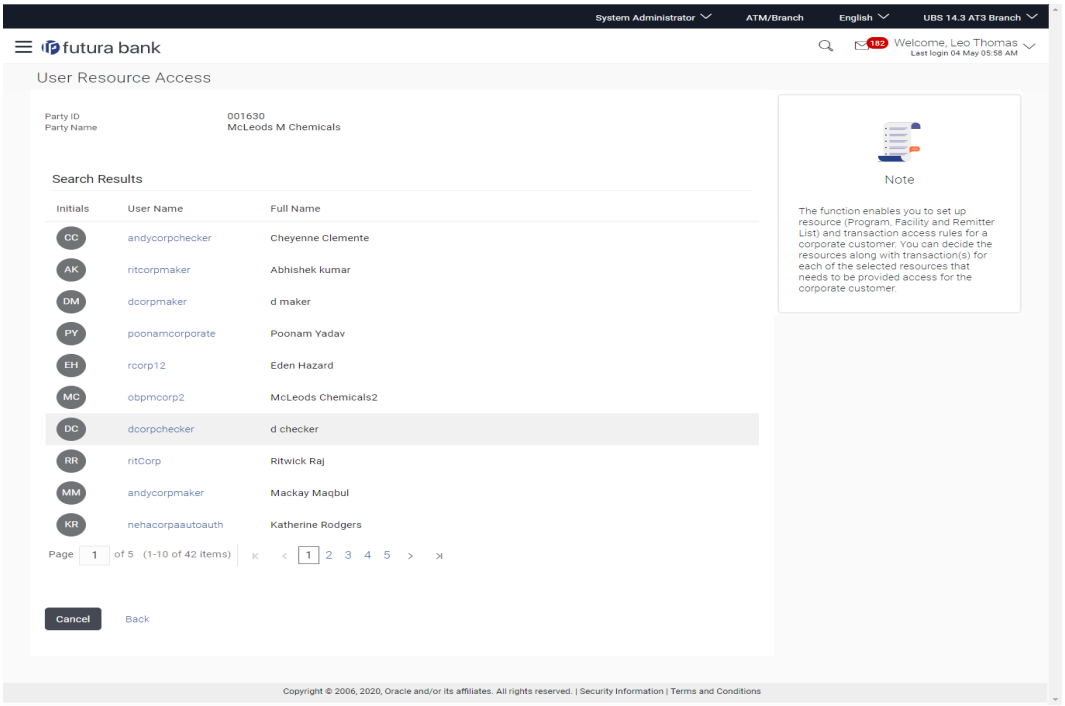
13.2 User Resource Access- Search

The Bank Administrator can view the list of remitter(s) and transactions for which access has been provided to the user.

To view the remitter and transaction access:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**.
   For a searched party, there will be a list of users displayed with information like user ID, full name of the user and initials of the user.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.

User Resource Access - Search Result



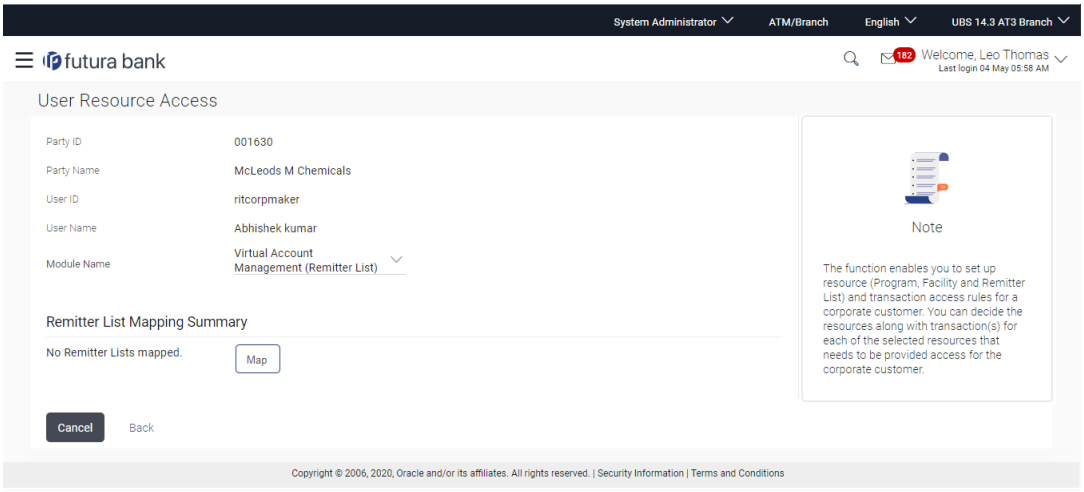
Field Description

Field Name	Description
Party ID	The party ID searched by the Bank Administrator.
Party Name	The name of the party.

Field Name	Description
Search Result	
Initials	Initials of the user.
User Name	User name of the user
Full Name	Full name of the user.

3. Click the **User Name** link against the user record for which you want to view the details. The **User Resource Access – Mapping Summary** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

User Resource Access – Summary Page



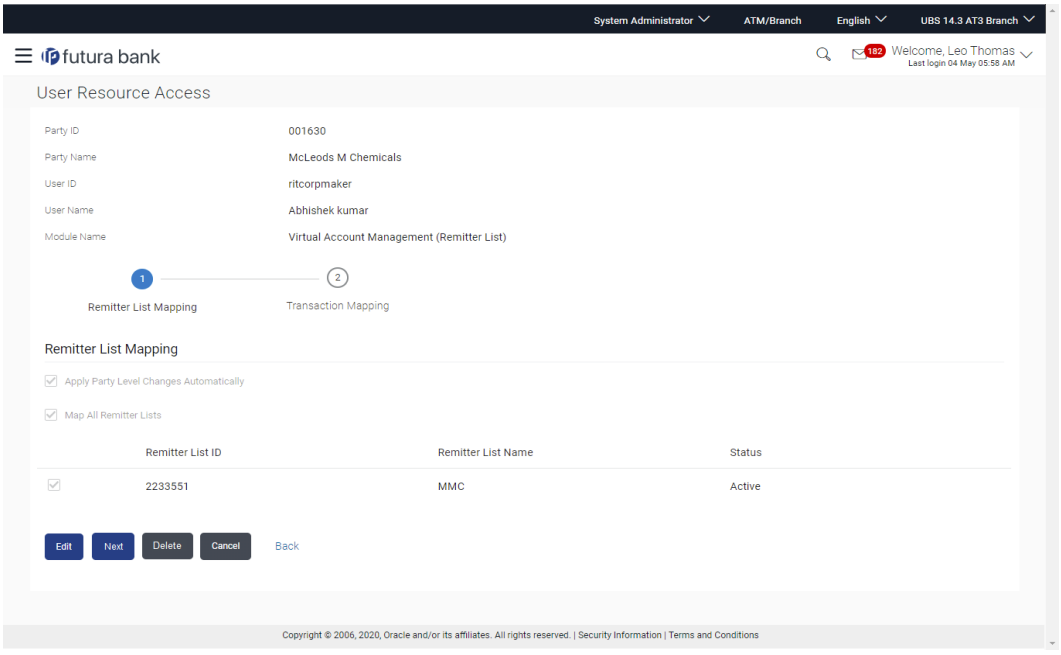
Field Description

Field Name	Description
Party ID	The party ID searched by the Bank Administrator.
Party Name	The name of the party.
User ID	User ID of the selected user.
User Name	User name of the selected user

Field Name	Description
Module Name	The name of the module.
Remitter List Mapping Summary	
Resource Type	The resource types available under the party. The resource type can be: • Remitter List
Total Number of Remitter Lists	Total number of remitter lists available under the party.
Number of Remitter Lists Mapped	Number of remitter lists mapped to the particular resource type.

4. Click the **Remitter List** link to view the remitter mapping. The **User Resource Access – View** screen, displaying remitter list mapping appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

User Resource Access – View

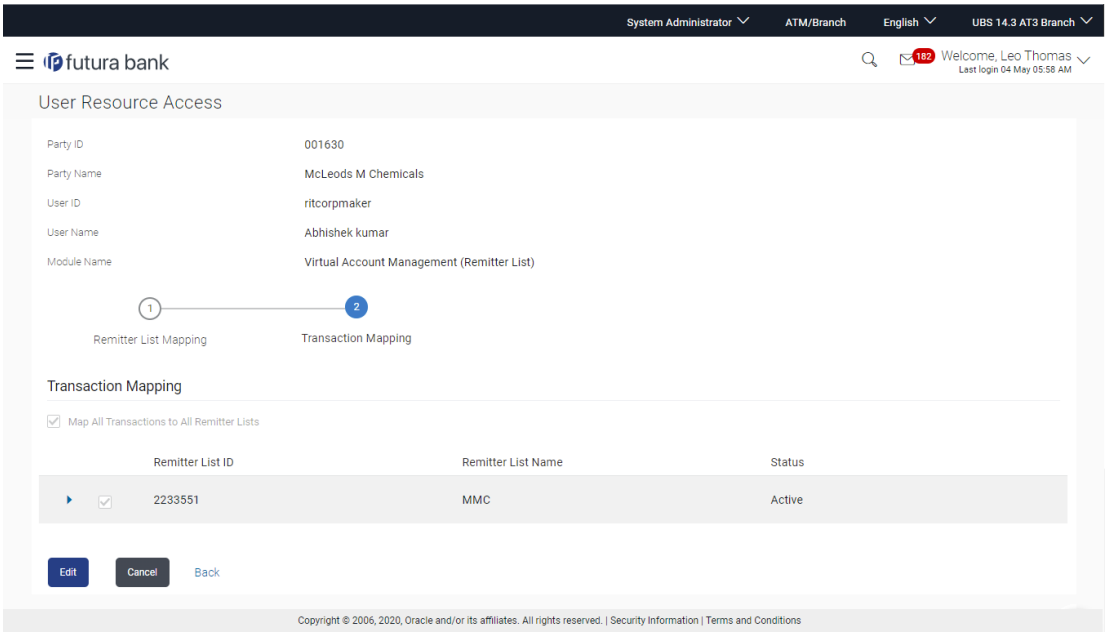


Field Description

Field Name	Description
Party ID	The party ID searched by the Bank Administrator.
Party Name	The name of the party.
User ID	User ID of the selected user.
User Name	User name of the selected user.
Module Name	The name of the module.
Remitter List Mapping	
Apply Party Level Changes Automatically	User will get access to remitter lists that are allowed/ disallowed at the party level.
Map All Remitter List	Mapping all the remitter lists to the user that are allowed at the party level.
Remitter List ID	Remitter List Identifier.
Remitter List Name	Name of the remitter list available under the party.
Status	Status of the remitter access for the party

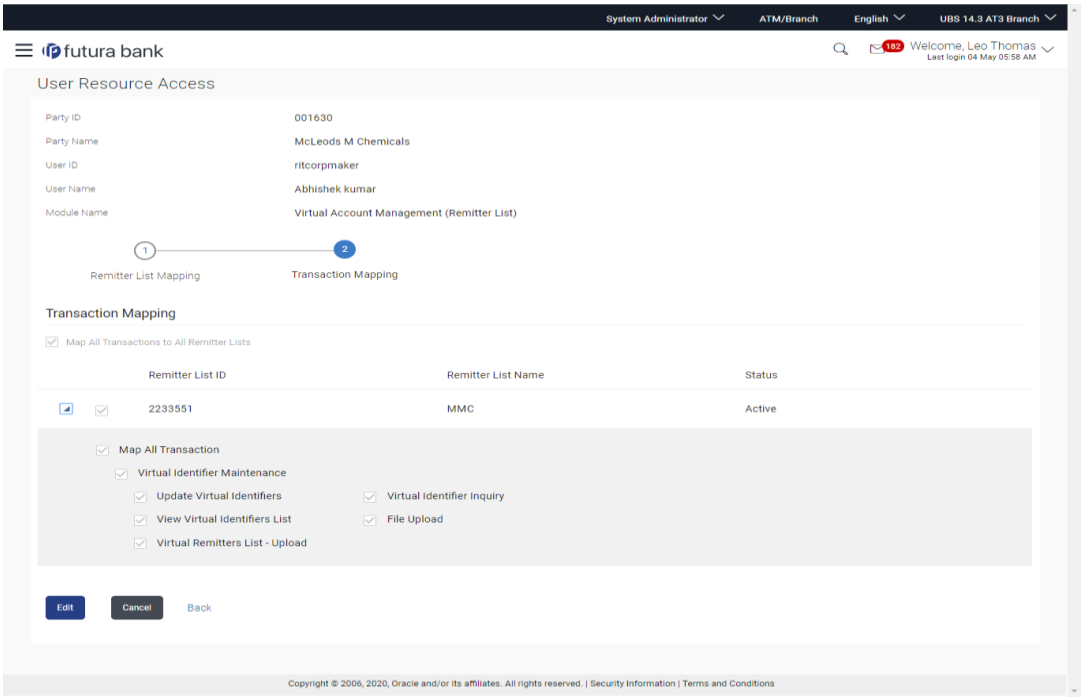
5. Click **Next**. The **User Resource Access – View (Transaction Mapping)** screen appears.
   OR
   Click **Edit** to modify the remitter list mapping.
   OR
   Click **Delete** to delete the User Resource Access setup.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

User Resource Access - Transaction Mapping - View



6. Click ▸ against the particular Remitter List to view the mapped transactions.
   OR
   Click **Edit** to update transaction mapping.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

User Resource Access - Transaction Mapping - View Mapping



7. Click **Edit** to update the User Resource Access mapping.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

13.3 User Resource Access - Edit

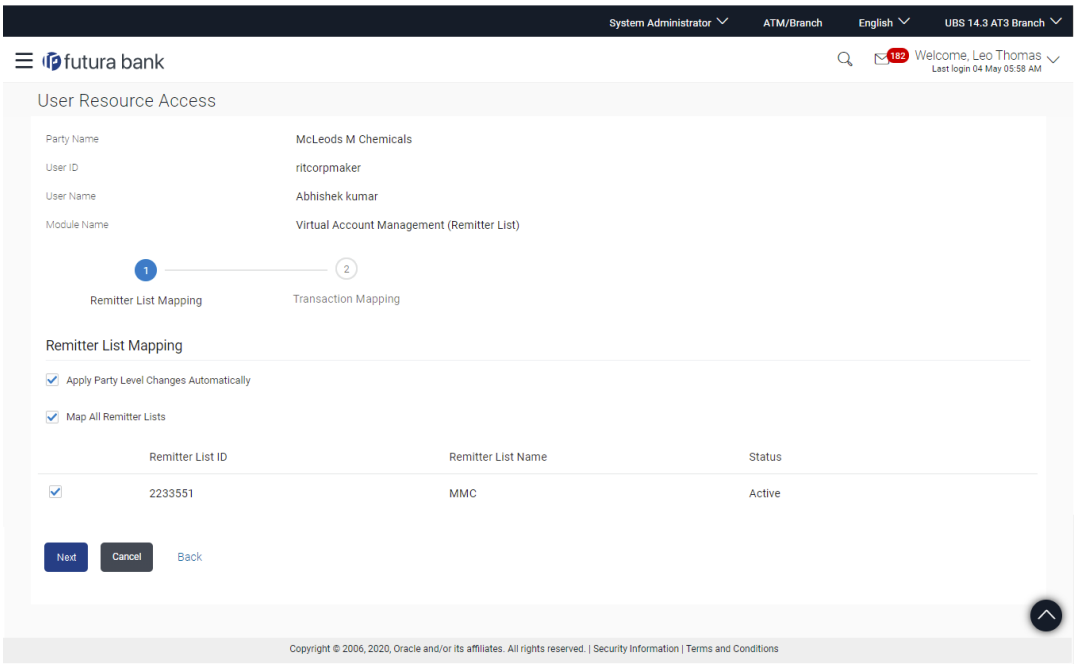
The Bank Administrator gets a request with the list of remitter lists and transactions for which access details needs to be edited for a selected user of the party.

To edit remitter list and transaction access for the user:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**.
   For a searched party, there will be a list of users displayed with information like user ID, full name of the user and initials of the user.
3. Click the **User Name** link against the user record for which you want to edit the details. The **User Resource Access – Mapping Summary** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

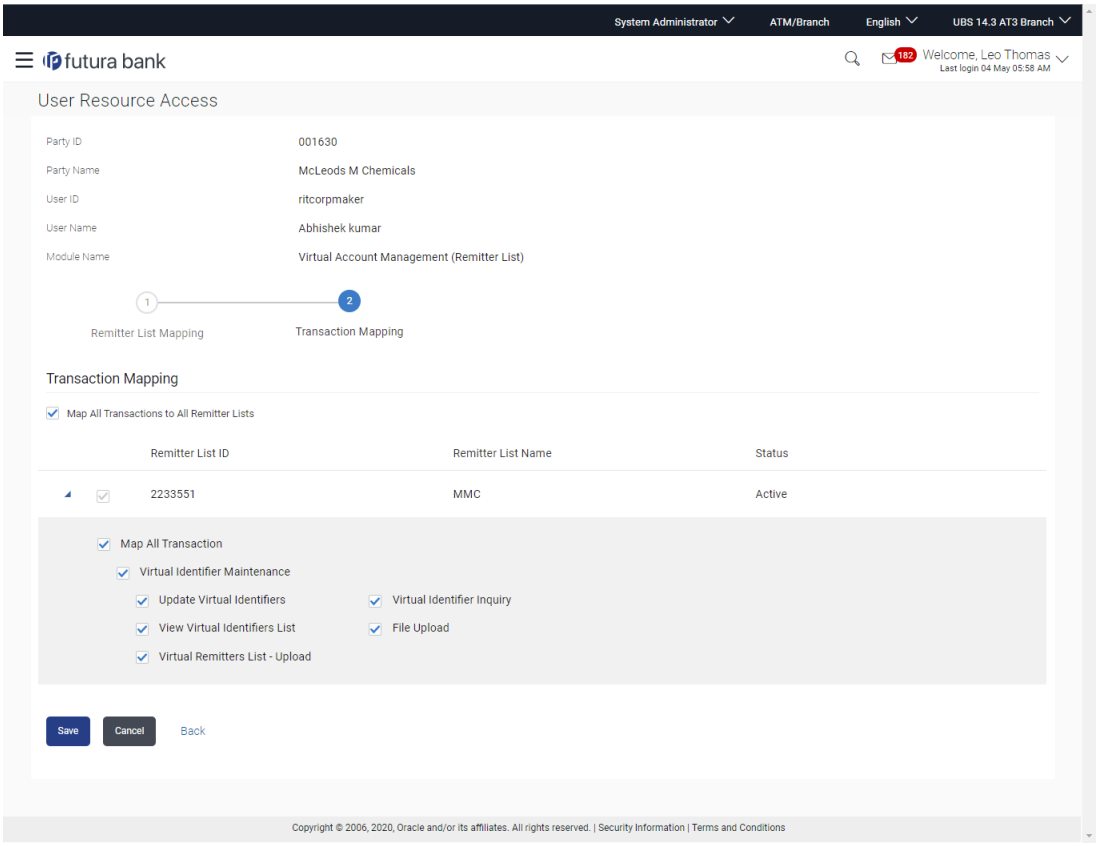
4. Click the **Remitter List** link. The **User Resource Access – View** screen, displaying remitter list mapping appears.
5. Click **Edit**. The **User Resource Access - Edit** screen appears.
   This enables the selection and de-selection option against the remitter list. There is also an option to edit check box **Apply Party Level Changes Automatically** to apply/ remove the party changes.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

User Resource Access – Edit



6. Select the respective check boxes preceding the **Remitter List ID** to be mapped.
   OR
   Select **Map All Remitter List**, if you want to map all the Remitter Lists available.
   Select/ De-select check box **Apply Party Level Changes Automatically** to apply/remove the party changes.
7. Click **Next**. The **User Resource Access - Edit** screen with mapped remitter list appears.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.
8. To map the transactions to the remitter lists, click ▸ against the particular Remitter List ID to view the transaction mapping.

User Resource Access - Transaction- Resource Mapping - Edit



9. Select the respective check boxes preceding the transaction to be mapped.
   OR
   Select **Map All Transactions**, if you want to map all the transactions to all Remitter Lists.
10. Click **Save**.
    OR
    Click **Back** to navigate to the previous screen.
    OR
    Click **Cancel** to cancel the transaction.
11. The **User Resource Access - Review** screen appears. Verify the details, and click Confirm.
    OR
    Click Edit to edit the transaction.
    OR
    Click Cancel to cancel the transaction.
12. The **User Resource Access - Confirmation** screen with success message appears along with the reference number and status of the transaction.
    Click OK to complete the transaction.

13.4 User Resource Access - Delete

The Bank Administrator gets a request with the user information of a party for which access details needs to be deleted. As part of this option, remitter list mapping can be deleted for a user.

To delete remitter and transaction access for the user:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the party name of the user.
2. Click **Search**.
   For a searched party, there will be a list of users displayed with information like user ID, full name of the user and initials of the user.
3. Click the **User Name** link against the user record for which you want to delete the details.
   The **User Resource Access – Mapping Summary** screen appears.
4. Click the **Remitter List** link. The **User Resource Access – View** screen, displaying remitter list mapping appears.
5. Click **Delete**. The application will prompt the administrator with a deletion message with an option of Yes / No.
   OR
   Click **Edit** to modify the remitter list mapping.
   OR
   Click **Next** to go to the next screen. The **User Resource Access – View (Transaction Mapping)** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
6. Click **Yes** to proceed with the deletion request. It will navigate to confirmation page with a success message and the status.
   OR
   Click **No** if you do not wish to proceed with deletion.
7. Click **OK** to complete the transaction.

14. Approvals

Each user is assigned a particular task to perform as per their position in the hierarchy of the bank. For instance, some user(s) may be given rights to do data entry for transactions such as domestic fund transfer, draft issuance by logging in to channel banking. Transaction created by initiator in the system is routed to the appropriate authorized signatory or group of signatories for approval depending upon the rules configured. A transaction once approved by all the required approvers gets processed.

Approval Management function enables the Bank Administrator to configure approval flows for various financial and non-financial transactions on channel banking for bank's customers, Business Parties and users and for administrators.

Approval flow includes configuration of rules for the users with following access types:

- Maker/ Initiator – User who is a creator of the transaction.
- Authorizer/ Approver – User who authorizes the transactions created by the maker. His authorization rights are maintained by an administrator.

Features supported in application

Approval management supported for Bank administrator users includes;

- Approval Workflow Maintenance
- Approval Rule Maintenance

14.1 Workflow Management

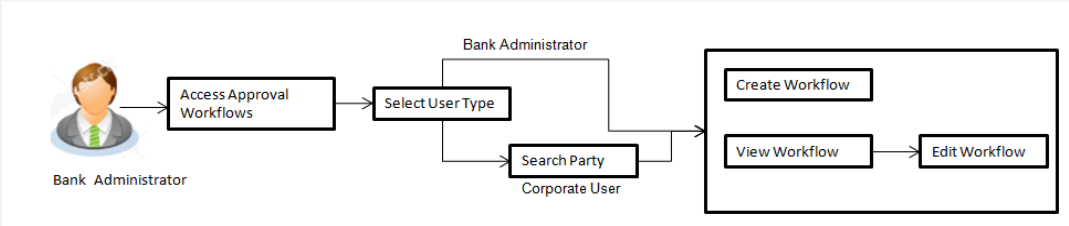
Approval workflows are created to support requirements where multiple levels of approval are required in a specific sequence for a transaction/maintenance. Each workflow can be configured to have up to five levels of approval with a specific user or a user group configured at each level.

Workflows can be created independently and can be attached to a specific transaction/maintenance as part of the Approval Rule configuration.

Prerequisites

- Transaction access is provided to Bank Administrator.
- Party preference is maintained.
- Multiple users are maintained under a party or as Bank Administrators
- Approval rule set up for Bank Administrator to perform the actions.
- Necessary user groups are maintained using User Group Management.

Workflow



Features supported in application

Approval Rule maintenance allows Bank Administrator to:

- View Approval Workflows
- Create Approval Workflows
- Edit Approval Workflows

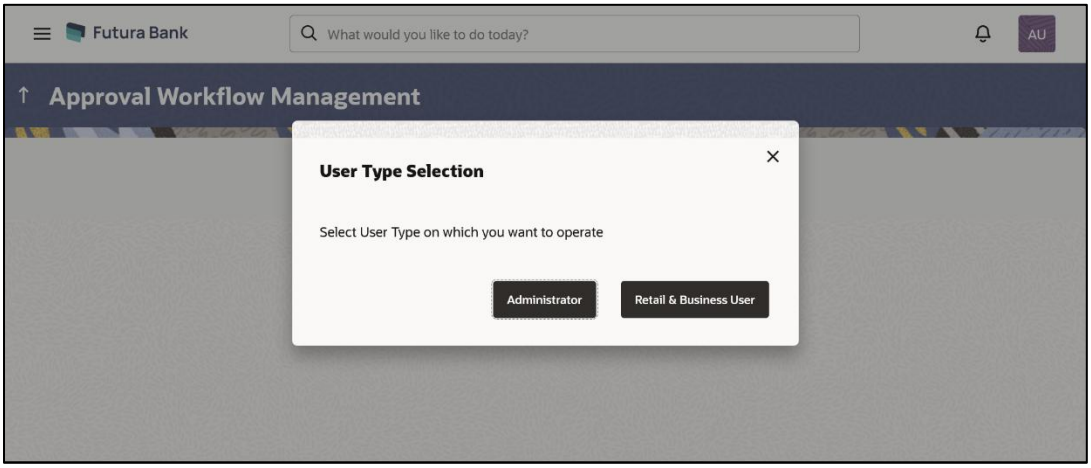
How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Approvals > Workflow Management

14.1.1 Approval Workflow – Select User Type

Bank Administrator logs into the system and navigates to the Approval Workflow screen. On accessing the 'Approval Workflow Management' menu, bank administrator has to select the user type for whom the workflows are to be maintained.

Approval Workflow – Select User Type

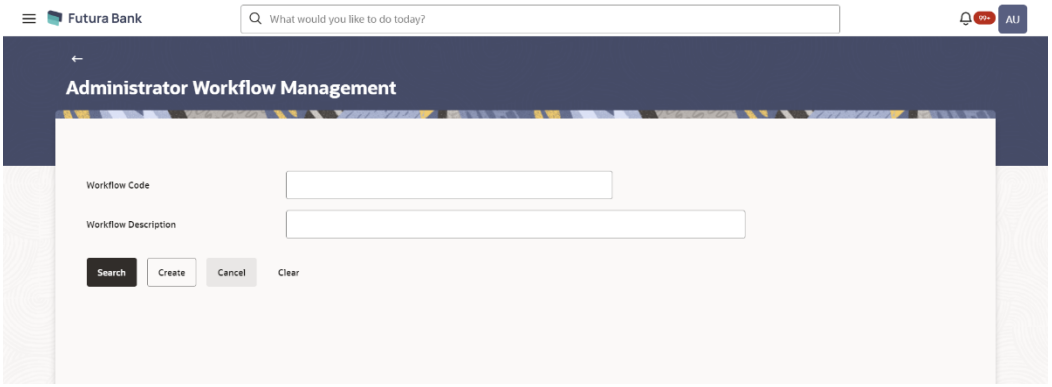


1. Click **Admin User** to access the workflow management of bank administrator users. The **Admin Workflow Management** screen appears.

2. Click **Retail & Business User** to access the workflow management for **Retail and Business** users. The **Workflow Management** screen appears.

14.1.2 Approval Workflow - Admin User - Workflow Management

Admin Workflow Management



Field Description

Field Name	Description
Workflow Code	Code of the already maintained approval workflow.
Workflow Description	Description of the already maintained approval workflow.

3. Click **Create** to create new admin workflow. The **Admin Workflow Management – Create** screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate the user back to 'Dashboard'.
   OR
   Enter the search parameters and click **Search** to search the matching records.
   OR
   Click **Clear** to clear the input search parameters.

14.1.2.1 Admin Workflow Management – Search

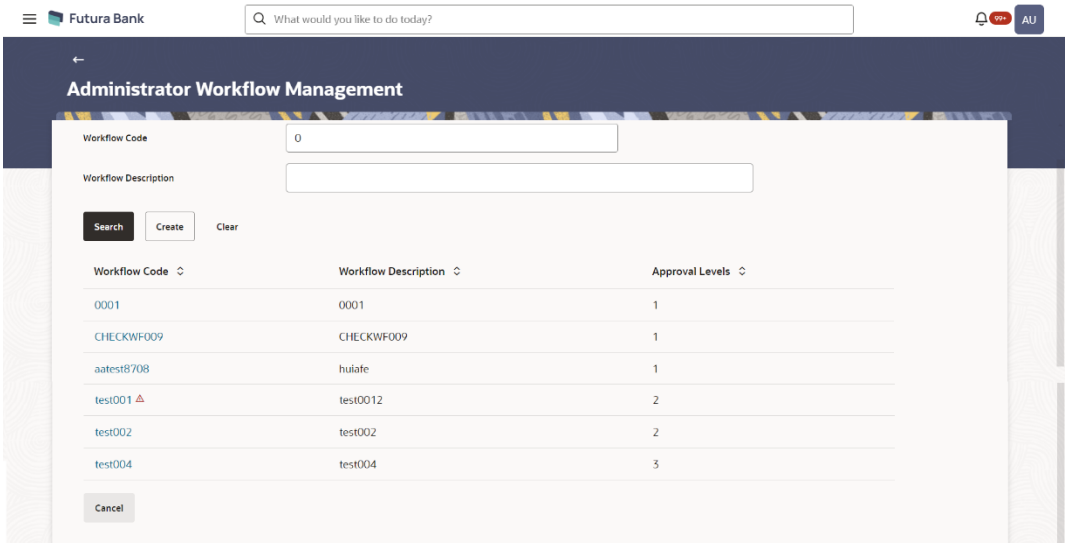
Bank Administrator user can search the workflows maintained for administrator users.

Workflows maintained (if any) for admin users are displayed on the screen after searching with valid input. User can view the details of existing workflow by clicking on the search results or can create new approval workflow using this screen.

To search the approval workflow for admin users:

1. In the **Admin Workflow Management** screen, enter the search parameters and click **Search**. The **Admin Workflow Management** screen with search results appears based on the searched criteria.

Admin Workflow Management – Search



Field Description

Field Name	Description
Workflow Code	The approval workflow code to search the approval workflows.
Workflow Description	The approval workflow description to search the approval workflows.
Search Results	
Workflow Code	Unique code of the already maintained approval workflow.
Workflow Description	Description of the already maintained approval workflow.
Approval Level	Number of approval levels in each workflow.

2. Click the **Work Flow code** link, to view details of the selected Approval Workflow. The **Workflow Management - View** screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Clear** to reset the data entered.

OR
Click **Create** to create new Approval Workflow for admin users.

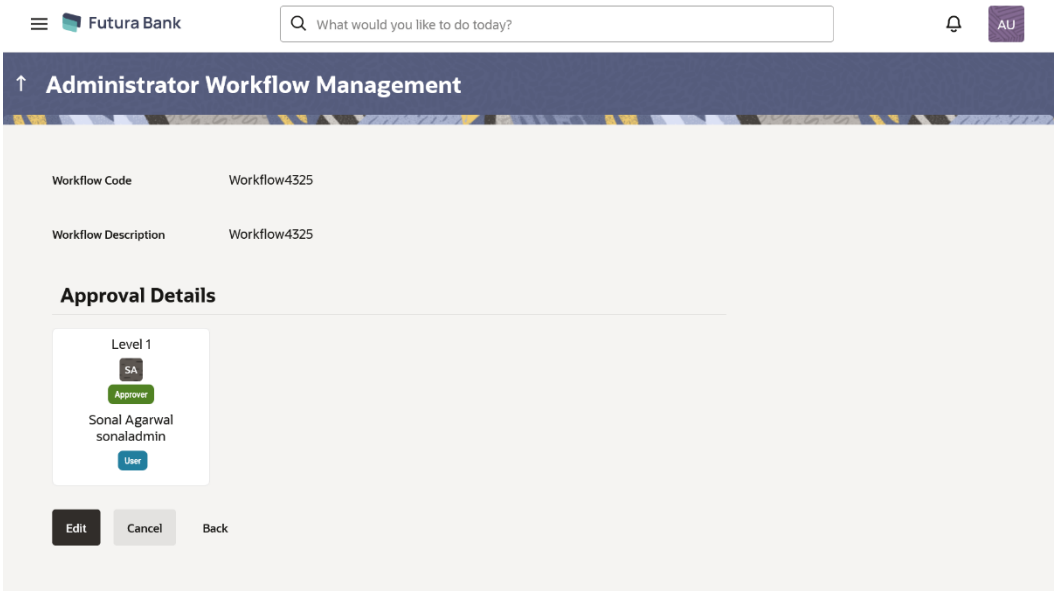
14.1.2.2 Admin Workflow Management – View

Further drill down is given on the each workflow to view the details of the users/ user groups who are the part of workflow.

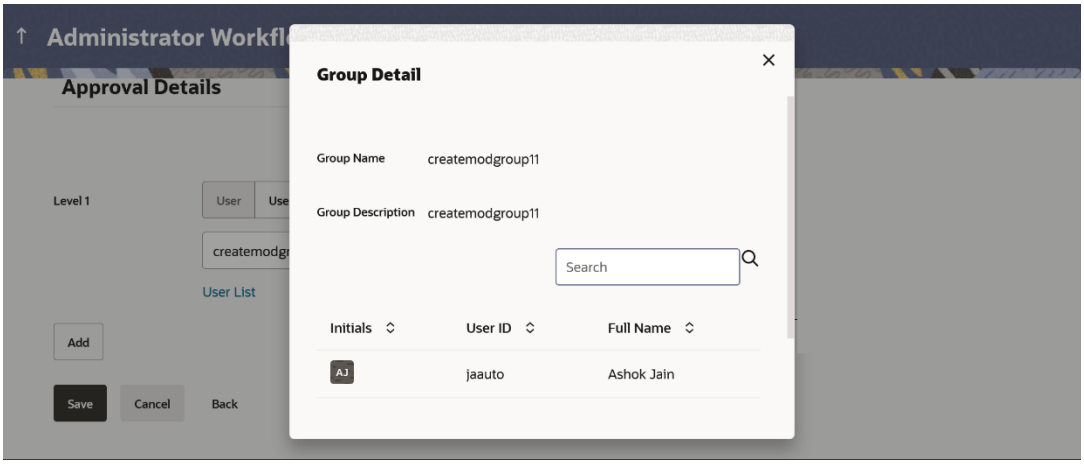
To view the approval workflow for corporate users:

3. In the **Admin Workflow Management** screen, enter the search parameters and click **Search**. The **Admin Workflow Management** screen with search results appears based on the searched criteria.
4. Click the **Work Flow code** link, to view details of the selected Approval Workflow. The **Workflow Management - View** screen appears.

Admin Workflow Management – View



Group Details



Field Description

Field Name	Description
View	
Workflow Code	Workflow code is displayed.
Workflow Description	Workflow description is displayed.

Field Name	Description
Approval Details	
Approval Level	User / user group maintained at each approval level. There can be up to five levels of approval levels.
User Name / User Groups	User or a user group maintained at each level of approval. On Approval -Workflow screen, Admin User can click on the Name of the user group that is part of the workflow to see the list of users which are part of that Group User can search specific user name, by using the search window on Group Details overlay.

5. Click **Edit** to edit the workflow. The **Admin Workflow Management - Edit** screen with values in editable form appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to the previous screen.

14.1.2.3 Admin Workflow Management – Create

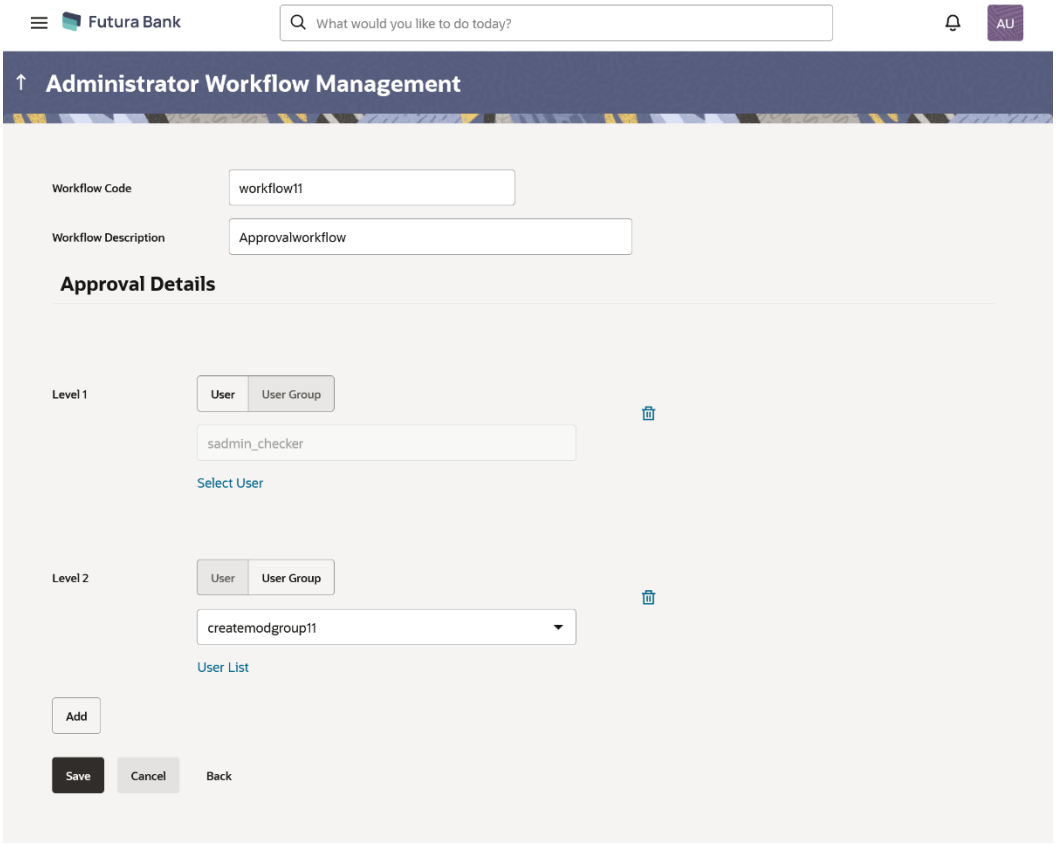
Bank Administrator can create approval workflows for the Admin users. By default, user can specify minimum one and maximum five levels of approvals as a part of workflow.

Administrator can set either an individual user or user group of a corporate as a part of each level of approval. Approval type (sequential/non-sequential/no authorization) is defined at the party preference.

To create an approval workflow:

1. In the **Admin Workflow Management** screen, click **Create**. The **Admin Workflow Management - Create** screen appears.

Admin Workflow Management – Create



Field Description

Field Name	Description
Create	
Workflow Code	To specify approval workflow code.
Workflow Description	To specify approval workflow description.
Approval Details	
Approval levels for a user / user group. You can click Add for multi level approval process.	
Approval Level	Approval levels for a user / user group. User can click Add for multi level approval process.
User / User Group	To select specific user or a user group at each level of approval.

2. In the **Workflow Code** field, enter the workflow code.

3. In the **Workflow Description** field, enter the name of the workflow.
4. In the **Approval Details** section, from the **Level 1** field, click appropriate user / user group.
5. From the **User Name / User Groups** list, select the approver user name.
6. Click **Add** to add the selected user/ user group at specific level of approval.
   OR
7. Click icon to remove specific approval level.
8. Click **Save** to save Approval Workflow.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to previous screen.
9. The **Admin Workflow Management - Create - Review** screen appears post necessary validations. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to go back to previous screen.
10. The success message of saving the created approval workflow appears along with the transaction reference number and status.
    Click **OK** to complete the transaction.

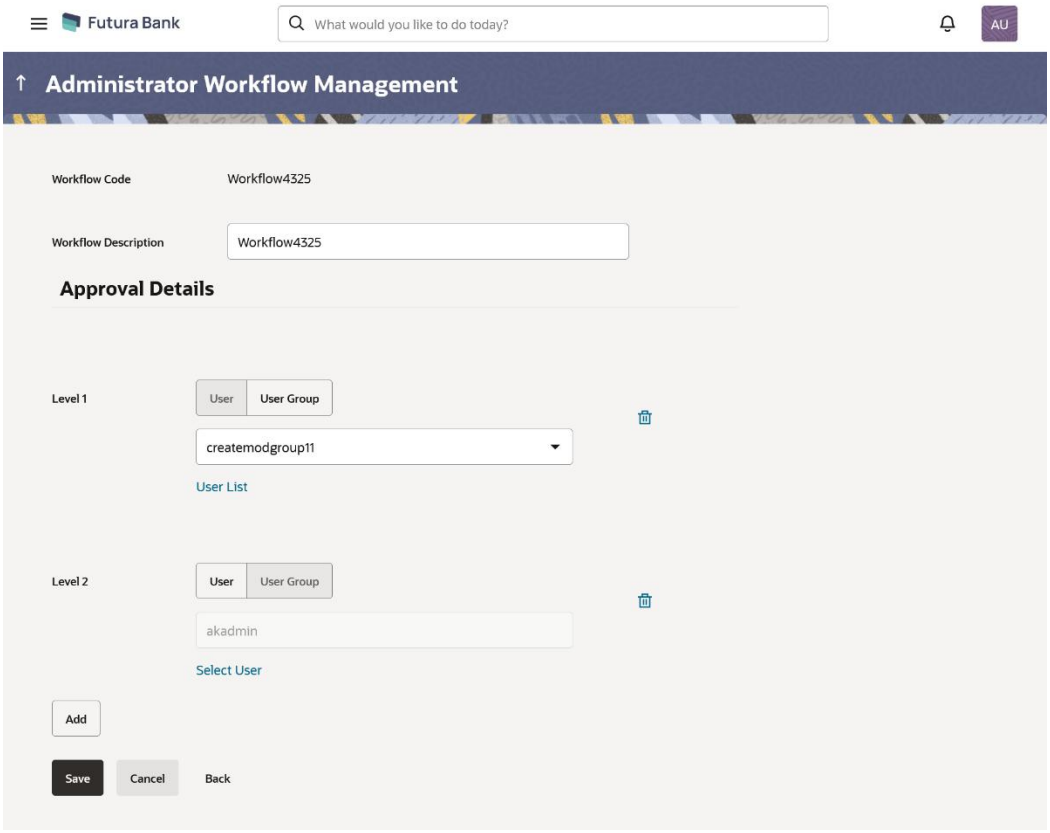
14.1.2.4 Admin Workflow Management - Edit

This function enables the Bank Administrator to update the description of the workflow and also to remove existing and add the new approval levels. Edited workflows are applicable for new transactions initiated post workflow update, whereas the previously initiated and transactions pending approval follows the old workflow.

To edit an approval workflow:

1. In the **Admin Workflow Management** screen, enter the search parameters and click **Search**. The **Admin Workflow Management** screen with search results appears based on the searched criteria.
2. In the **Admin Workflow Management** screen, click the **Work Flow code** link, for which you want to view the details. The **Admin Workflow Management - View** screen appears.
3. Click **Edit**. The **Admin Workflow Management - Edit** screen appears.

Admin Workflow Management - Edit



Field Description

Field Name	Description
Edit	
Workflow Code	Workflow code is displayed.
Workflow Description	Workflow description is displayed in editable form.
Approval Details	
Approval Level	Approval levels for a user / user group. Administrator can remove or add approval levels in a workflow.
User Name / User Groups	User or a user group maintained at each level of approval. Administrator can edit an existing user/user group maintained at each level and can also specify user/user group for additional approval level.

4. Edit the required details.
5. Click **Add** to add the selected user/ user group at specific level of approval.
   OR
   Click icon to remove specific approval level.
6. Click **Save** to save Approval Workflow.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to previous screen.
7. The **Admin Workflow Management – Edit - Review** screen appears post necessary validations. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation.
   OR
   Click **Back** to go back to previous screen.
8. The success message of saving the approval workflow modification appears along with the transaction reference number and status.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

14.1.3 Approval Workflow - Retail & Business User - Workflow Management

System displays a screen to enter the party information (party ID or party name) and search party for which the approval workflows are to be maintained/ viewed.

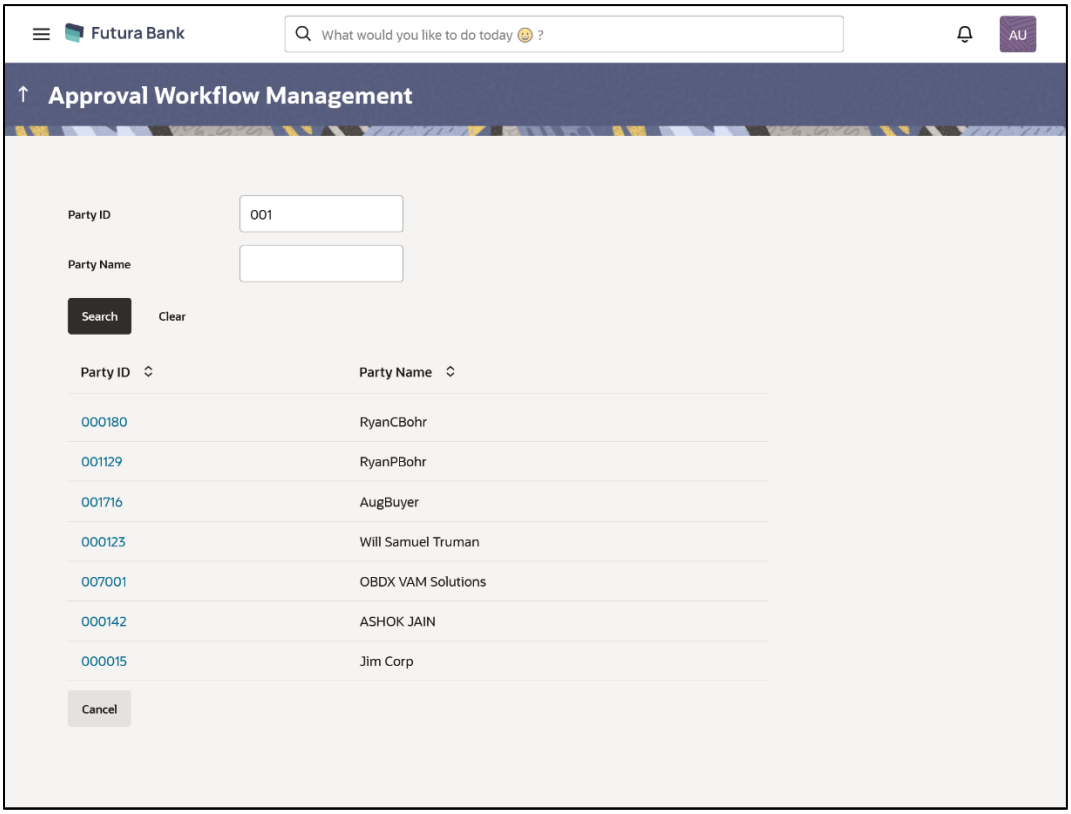
User can enter the party ID (if known) or the party name with a minimum of five characters.

System matches the input provided by the user with the party name records and displays the matching party records.

In case of a party search by party ID, it is an exact match and system displays the workflows maintained if any.

In case of a party search by name, system displays the matching party records. The records have parties listed with both Party ID and Party Name information. User can select the record by clicking on the Party ID from the list.

Workflow Management



Field Description

Field Name	Description
Party ID	Party ID to be searched.

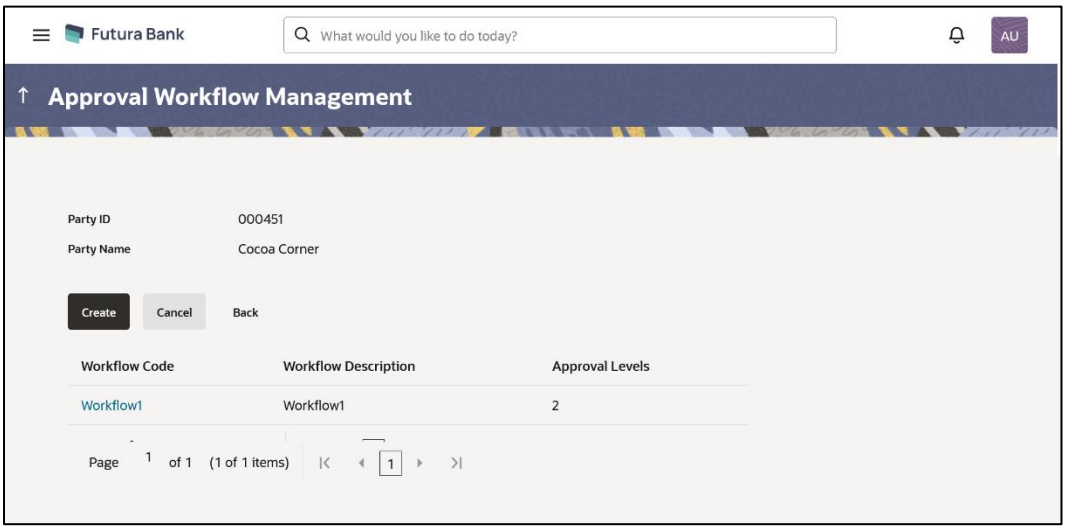
Field Name	Description
Party Name	Party name of the party ID to be searched.
Search Result	
Party ID	Party IDs as per search input. Click on the link to view workflows maintained under the party.
Party Name	Party name of the party ID.

1. Enter the search parameters and click **Search** to search the matching records.
   OR
   Click **Cancel** to cancel the operation and navigate the user back to 'Dashboard'.
   OR
   Click on '**Clear**' to clear the input search parameters.
2. Click on the **Party ID** link to view the workflows maintained under the selected party.

14.1.3.1 Retail & Business Workflow Management – Summary

Clicking on **Workflow Code** hyperlink, workflows maintained (if any) under a party are displayed on the screen. User can opt to view the details of existing workflows or can create new approval workflow using this screen.

Workflow Management – Summary



Field Description

Field Name	Description
Party ID	Party ID of which workflows to be viewed/ edited.
Party Name	Party name of Party ID of which workflows to be viewed/ edited.
Workflow Code	Code of the already maintained approval workflow. This field will be displayed only if there are existing approval workflows available under a party.
Workflow Description	Description of the already maintained approval workflow. This field will be displayed only if there are existing approval workflows available under a party
Approval Levels	Number of approval levels in each workflow. This field will be displayed only if there are existing approval workflows available under a party.

9. Click the **Workflow Code** link to view details of the selected Approval Workflow. The **Workflow Management - View** screen appears.
   OR
   Click **Create**. The **Workflow Management - Create** screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to previous screen.

14.1.3.2 Retail & Business Workflow Management – View

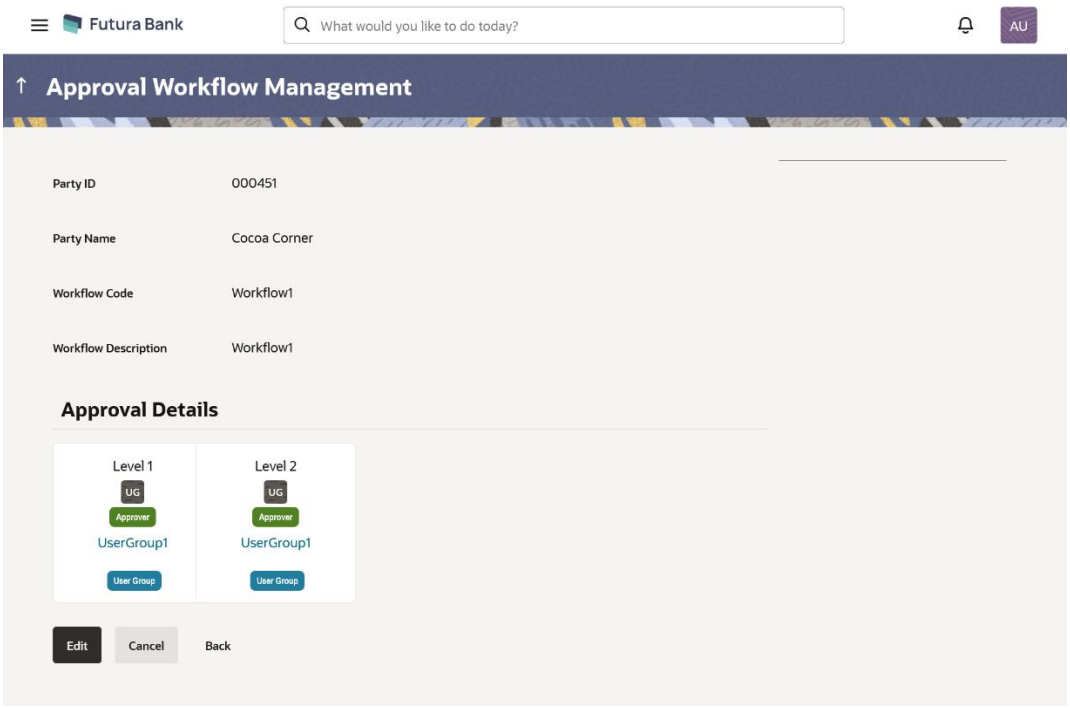
Further drill down is provided on the each workflow to view the details of the users/ user groups who are the part of workflow.

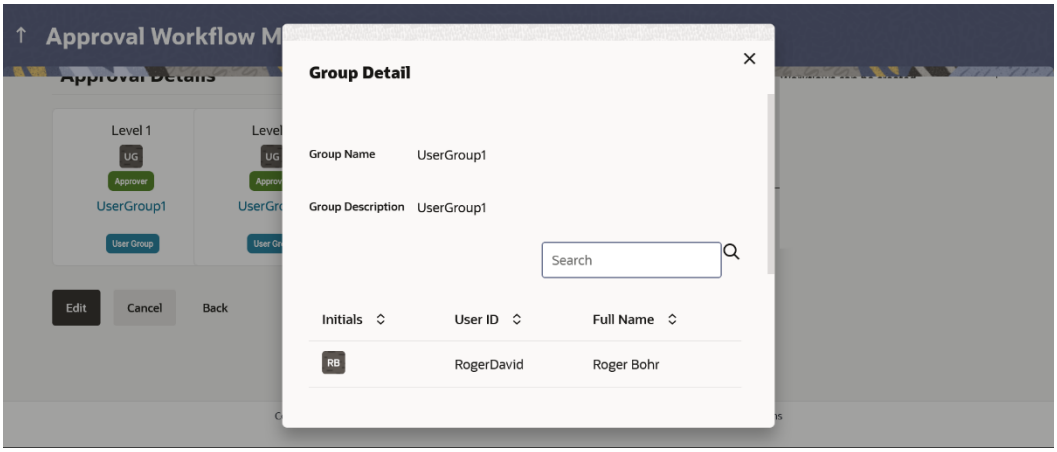
To view the approval workflow for retail and business users:

1. In the **Workflow Management** screen, enter the party id in the In the **Party Id** field.
   OR
   In the **Party Name** field, enter the party name.
2. Click **Search**. The **Workflow Management** screen with both Party ID and Party Name appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.
3. In the **Workflow Management** screen, enter the search parameters and click **Search**. The **Workflow Management** screen with search results appears based on the searched criteria.

4. Click the **Workflow Code** link to view details of the selected Approval Workflow. The **Workflow Management - View** screen appears.

Workflow Management – View





Field Description

Field Name	Description
View	
Party ID	Party ID of which workflows to be viewed/ edited.
Party Name	Party name of Party ID of which workflows to be viewed/ edited.
Workflow Code	Workflow code is displayed.
Workflow Description	Workflow description is displayed.
Approval Details	
Approval Level	User / user group maintained at each approval level.
User / User Group	User or a user group maintained at each level of approval. On Approval -Workflow screen, Admin User can click on the Name of the user group that is part of the workflow to see the list of users which are part of that Group User can search specific user name, by using the search window on Group Details overlay.

5. Click **Edit** to edit the workflow. The **Workflow Management - Edit** screen with values in editable form appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to the previous screen.

14.1.3.3 Retail & Business Workflow Management – Create

Bank Administrator can create approval workflows for retail and business users. By default, user can specify minimum one and maximum five levels of approvals as a part of workflow.

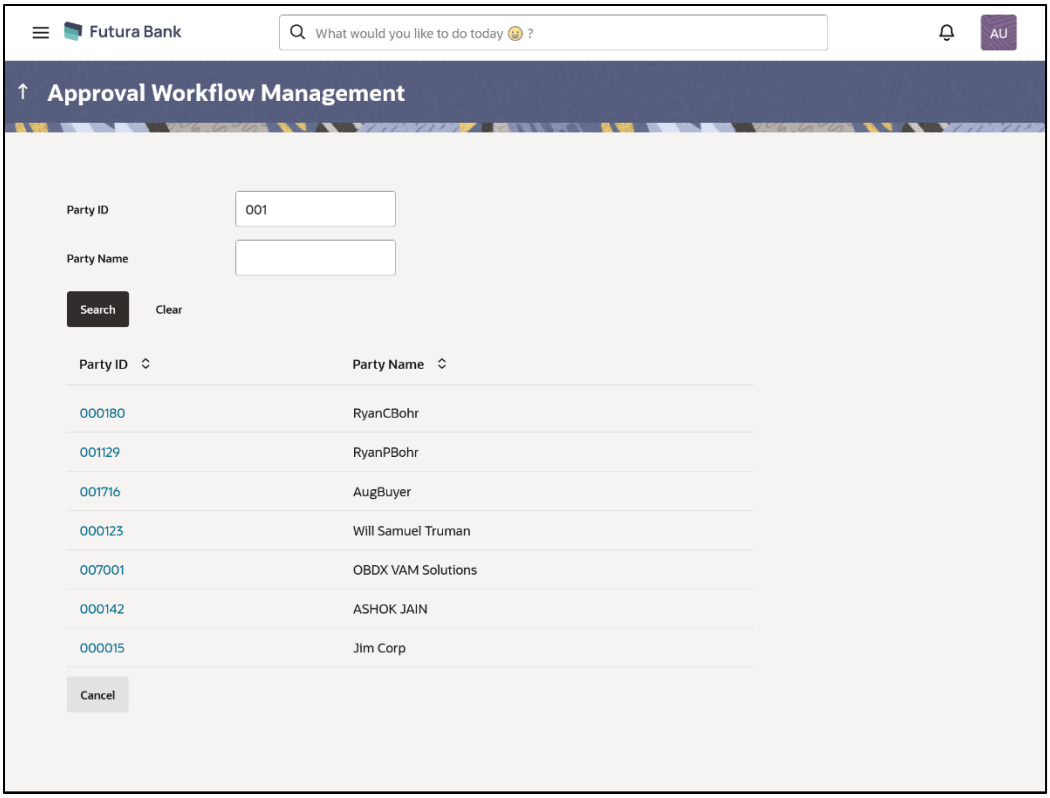
Administrator can set either an individual user or user group of a retail and business as a part of each level of approval. Approval type (sequential/non-sequential/no authorization) is defined at the party preference.

To create an approval workflow:

1. In the **Workflow Management** screen, enter the party id in the In the **Party Id** field.
   OR
   In the **Party Name** field, enter the party name.

2. Click **Search**. The **Workflow Management** screen with both Party ID and Party Name appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.

Workflow Management – Party Search

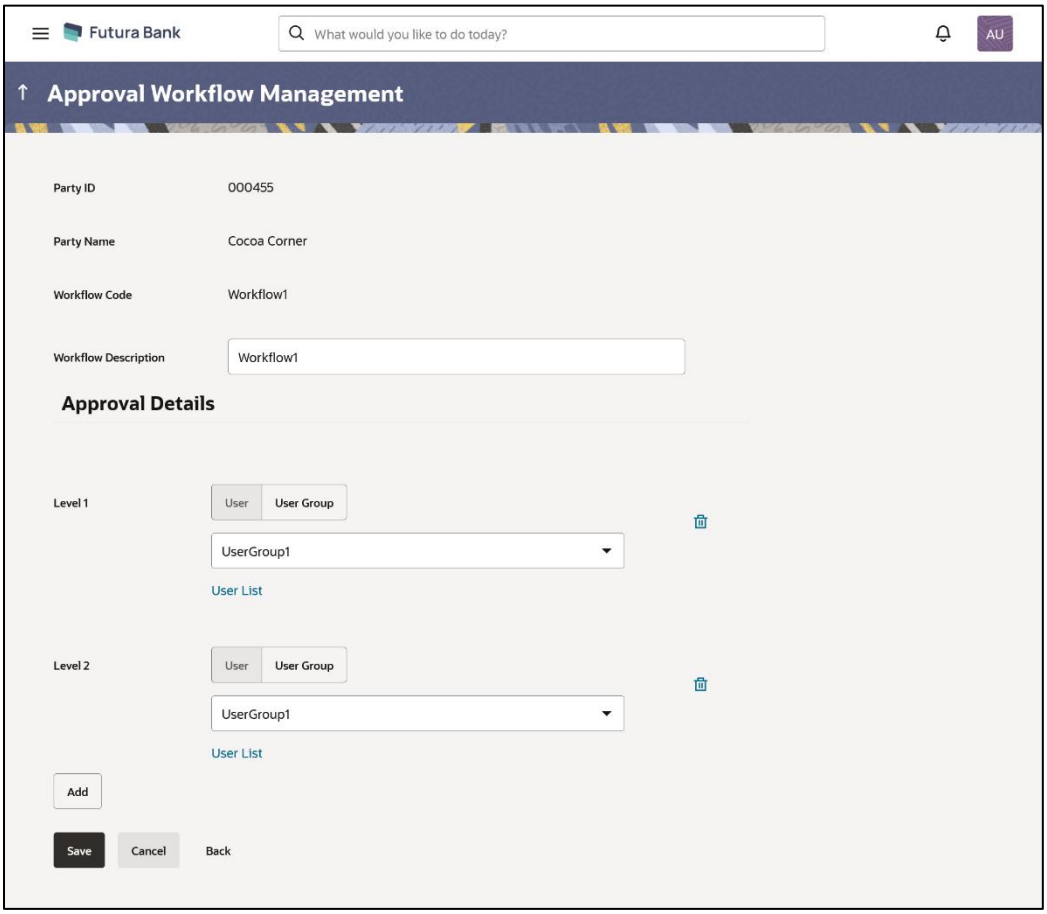


Field Description

Field Name	Description
Party ID	Party ID to be searched.
Party Name	Party name of the party ID to be searched.
Search Result	
Party ID	Party IDs as per search input. Click on the link to view workflows maintained under the party.
Party Name	Party name of the party ID.

3. Enter the search parameters and click **Search** to search the matching records.
   OR
   Click **Cancel** to cancel the operation and navigate the user back to 'Dashboard'.
   OR
   Click on '**Clear**' to clear the input search parameters.
4. Click on the **Party ID** link to view the workflows maintained under the selected party.
5. Click **Create**. The **Workflow Management - Create** screen appears.
   OR
   Click the **Workflow Code** link to view details of the selected Approval Workflow. The **Workflow Management - View** screen appears.

Workflow Management – Create



Field Description

Field Name	Description
Create	
Party ID	Party ID of which workflows to be viewed/ edited.

Field Name	Description
Party Name	Party name of Party ID of which workflows to be viewed/ edited.
Workflow Code	To specify approval workflow code.
Workflow Description	To specify approval workflow description.
Approval Details	
Approval Level	Approval levels for a user / user group. User can click Add for multi level approval process.
User / User Group	To select specific user or a user group at each level of approval.

6. In the **Workflow Code** field, enter the workflow code.
7. In the **Workflow Description** field, enter the name of the workflow.
8. In the **Approval Details** section, from the **Level 1** field, click appropriate user / user group.
9. From the **User Name / User Groups** list, select the approver user name.
10. Click **Add** to add the selected user/ user group at specific level of approval.
    OR
11. Click icon to remove specific approval level.
12. Click **Save** to save Approval Workflow.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
    OR
    Click **Back** to go back to previous screen.
13. The **Workflow Management - Create - Review** screen appears post necessary validations. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
    OR
    Click **Back** to go back to previous screen.
14. The success message of saving the created approval workflow appears along with the transaction reference number and status.
    Click **OK** to complete the transaction and navigate back to 'Dashboard'.

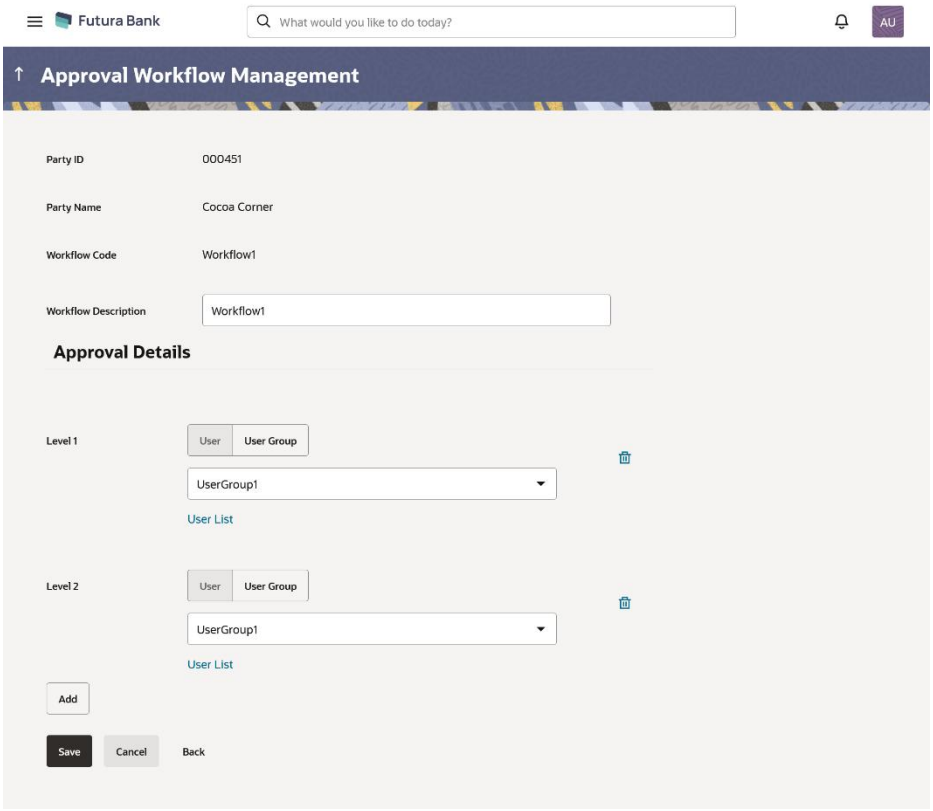
14.1.3.4 Retail & Business Workflow Management - Edit

This function enables the Bank Administrator to update the description of the workflow and also to remove existing and add the new approval levels. Edited workflows are applicable for new transactions initiated post workflow update, whereas the previously initiated and transactions pending approval follows the old workflow.

To edit an approval workflow:

1. In the **Workflow Management** screen, enter the party id in the In the **Party Id** field.
   OR
   In the **Party Name** field, enter the party name.
2. Click **Search**. The **Workflow Management** screen with both Party ID and Party Name appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.
3. In the **Workflow Management** screen, enter the search parameters and click **Search**. The **Workflow Management** screen with search results appears based on the searched criteria.
4. Click the **Workflow Code** link to view details of the selected Approval Workflow. The **Workflow Management - View** screen appears.
5. Click **Edit** to edit the workflow. The **Workflow Management - Edit** screen with values in editable form appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to go back to the previous screen.

Workflow Management - Edit



Field Description

Field Name	Description
Edit	
Party ID	Party ID of which workflows to be viewed/ edited.
Party Name	Party name of Party ID of which workflows to be viewed/ edited.
Workflow Code	Workflow code is displayed.
Workflow Description	Workflow description is displayed in editable form.
Approval Details	
Approval Level	Approval levels for a user / user group. Administrator can remove or add approval levels in a workflow.

Field Name	Description
User Name / User Groups	User or a user group maintained at each level of approval. Administrator can edit an existing user/user group maintained at each level and can also specify user/user group for additional approval level.

6. Edit the required details.
7. Click **Add** to add the selected user/ user group at specific level of approval.
   OR
   Click icon to remove specific approval level.
8. Click **Save** to save Approval Workflow.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to cancel the operation and go back to previous screen.
9. The **Workflow Management - Edit- Review** screen appears post necessary validations. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to cancel the operation and go back to previous screen.
10. The success message of saving the approval workflow modification appears along with the transaction reference number and status.
    Click **OK** to complete the transaction and navigate back to 'Dashboard'.

FAQ

1. **What is approval management?**

   Approval Management enables a bank administrator to set up approval conditions for various transactions on channel banking. The approval management allows setting up the maker / checker flow, wherein a transaction is initiated by a maker and the same is authorized by a single / multiple checkers depending on the configuration.

2. **What is approval workflow maintenance?**

   Approval workflows are created to support requirements where multiple levels of approval are required in a specific sequence for a transaction/maintenance. Each workflow can be configured to have up to 5 levels of approval with a specific user or a user group configured at each level.

3. **How many approval levels can I set up in the system?**

   Administrator can set up minimum one and maximum five levels of approvals as a part of approval workflow.

4. **Can I get the list of users associated with a group from workflow management screen?**

   No, list of the users associated with a group cannot be viewed using workflow management screen. However you can view the same from User Group Management screen.

14.2 Approval Rules

This function enables the Bank Administrator to set up conditions for approval as per the bank/corporate requirements. Rule can be set up for financial transactions, non-financial, non account financial transactions, and for maintenances. Flexibility exists to define approval rules with conditions stating that 'specific transaction' if initiated by a 'specific user/ user group' has to be approved by a 'specific approver/approver group' along with other attributes like amount range etc.

Prerequisites:

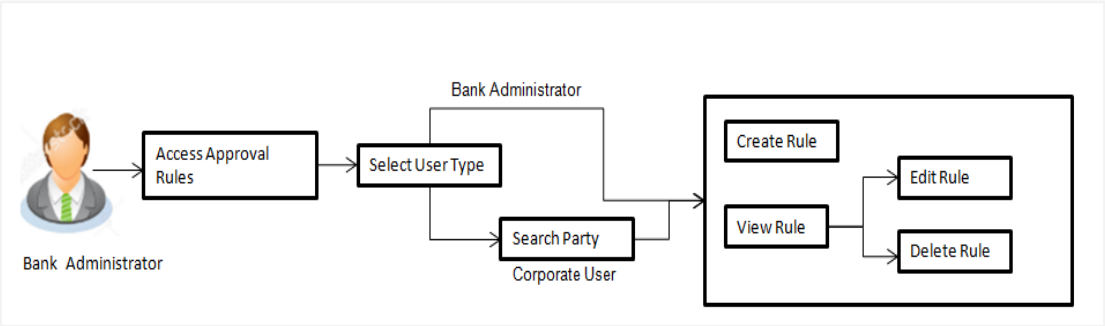
- Transaction access is provided to Bank Administrator
- Party preference is maintained for setting up rules for corporates
- Corporate and Administrator users are maintained
- Workflow configuration is maintained if approval required is to be set as 'Yes'
- Approval rule set up for Bank Administrator to perform the actions
- Necessary user groups and approval workflows are maintained

Features supported in application

The Approval Rule maintenances allow the bank administrator to:

- Create Approval Rules
- View Approval Rules
- Edit Approval Rules
- Delete Approval Rules

Workflow



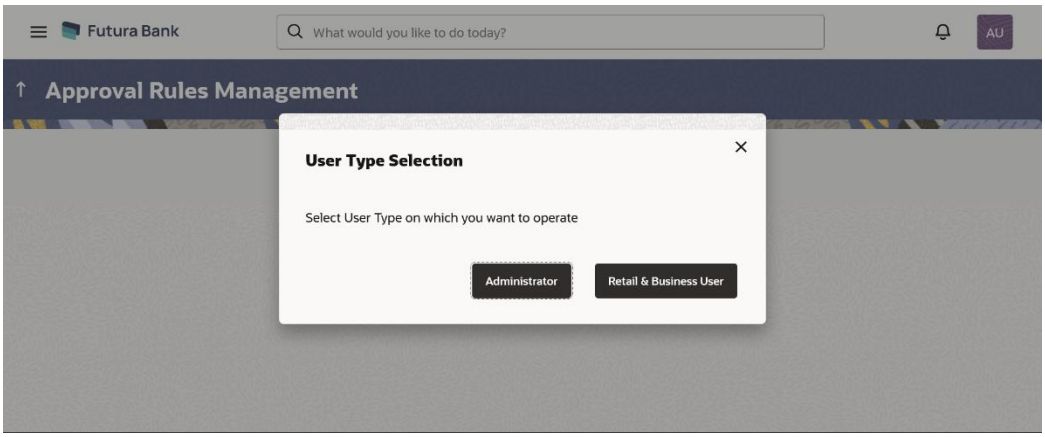
How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Approvals > Rule Management > Approval Rules

14.2.1 Approval Rules – Select User Type

Bank Administrator logs into the system and navigates to the Rule Management screen. On accessing the 'Approval Rules Management' menu, Bank Administrator has to select the user type for which the rules are to be maintained.

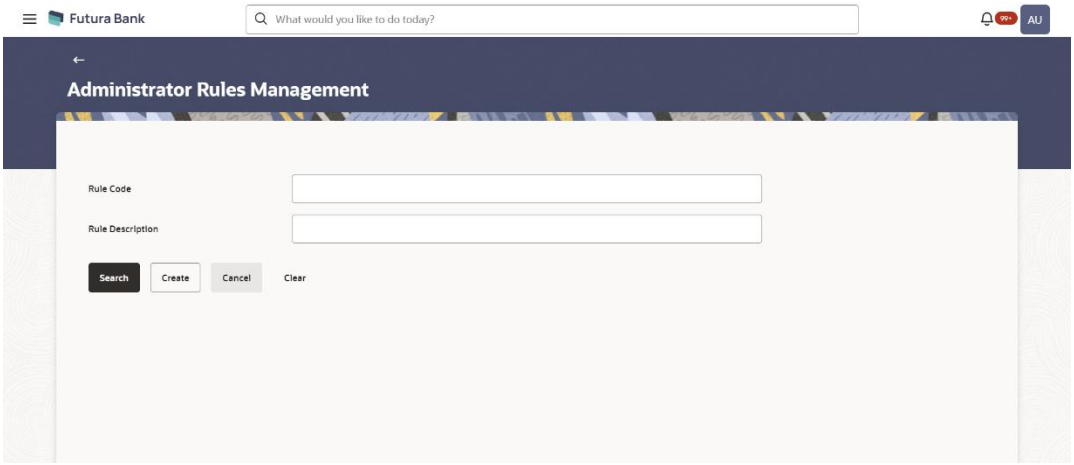
Approval Rules – Select User Type



1. Click **Admin User** to access the Approval Rules of Bank Administrator users. The **Admin Approval Rules** screen appears.
2. Click **Retail & Business User** to access the Approval Rules for **Retail and Business** users. The **Approval Rules** screen appears.

14.2.2 Approval Rules - Admin User - Approval Rules

Admin Approval Rules



Field Description

Field Name	Description
Rule Code	Search rules with a rules code of the already maintained approval rule.
Rule Description	Search rules with a rule description of the already maintained approval rule.

3. Click **Create** to create new admin workflow. The **Admin Approval Rules – Create** screen appears.
   OR
   Enter the search parameters and click **Search** to search the matching records.
   OR
   Click **Cancel** to cancel the transaction'.
   OR
   Click on '**Clear**' to clear the input search parameters.

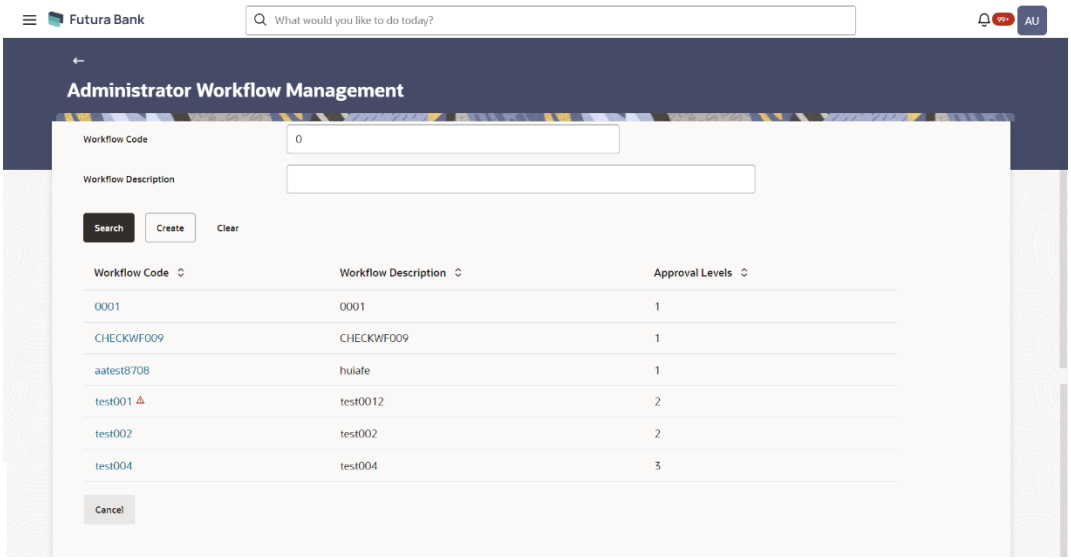
14.2.2.1 Admin Approval Rules – Search

Approval rules maintained (if any) for administrator users are displayed on the screen after searching with valid input. User can to view the details of existing rule or can create new approval rule using this screen.

To search the approval rules for admin users:

1. In the **Admin Approval Rules** screen, enter the search parameters and click **Search**. The **Admin Approval Rules** screen with search results appears based on the searched criteria.

Admin Approval Rules – Search



Field Description

Field Name	Description
Search Results	
Rule Code	Code of the already maintained approval rule.
Rule Description	Description of the already maintained approval rule.

2. Click the **Rule code** link, to view details of the selected Approval Rule. The **Approval Rules - View** screen appears.
   OR
   Click **Create** to create new Approval Rules for admin users.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to go back to previous screen.

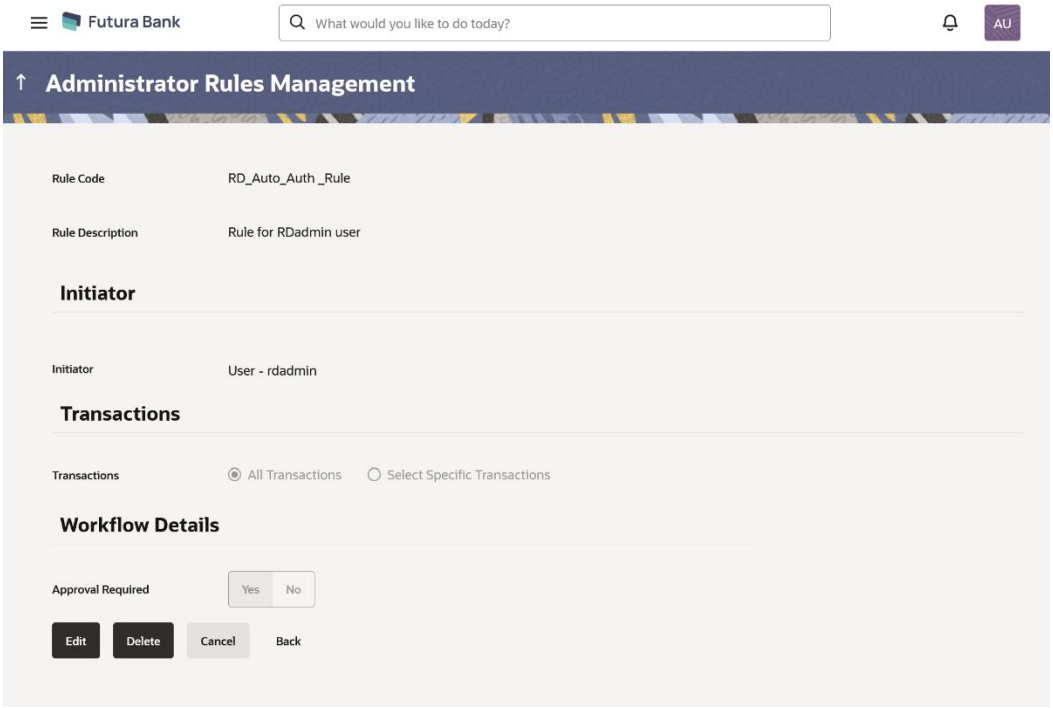
14.2.2.2 Admin Approval Rules – View

Further drill down is given on the each workflow to view the details of the users/ user groups who are the part of workflow.

To view the admin approval rules:

1. In the **Admin Approval Rules** screen, click the **Rule Code** link, for which user wants to view the details. The **Admin Approval Rules - View** screen appears.

Admin Approval Rules - View



Field Description

Field Name	Description
View	
Rule Code	Approval rule code.
Rule Description	Approval rule description.
Initiator	
Initiator Type	Initiator type specified while creating a rule.
User Name / User Groups	Name of the user or user group defined as initiator for the rule condition.
Transactions	Transaction for which the rule is set up.
Workflow Details	
Approval Required	Field displays whether approval is required or not for the set condition.
Workflow Details	Field displays the approval workflow details along with the defined approval levels. This field appears if you select **Yes** in the **Approval Required** field.

2. Click **Edit** to edit the approval rule. The **Admin Approval Rule - Edit** screen with values in editable form appears.
   OR
   Click **Delete** to delete the approval rule.
   The application will prompt the administrator with a deletion message, Click **Yes** to confirm.
   User is directed to **Admin Approval Rule – Delete** confirmation page
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to go back to previous screen..

14.2.2.3 Admin Approval Rules – Create

Approval rules can be setup based on the following parameters.

- Transactions
- Initiator
- Specific User
- User Group

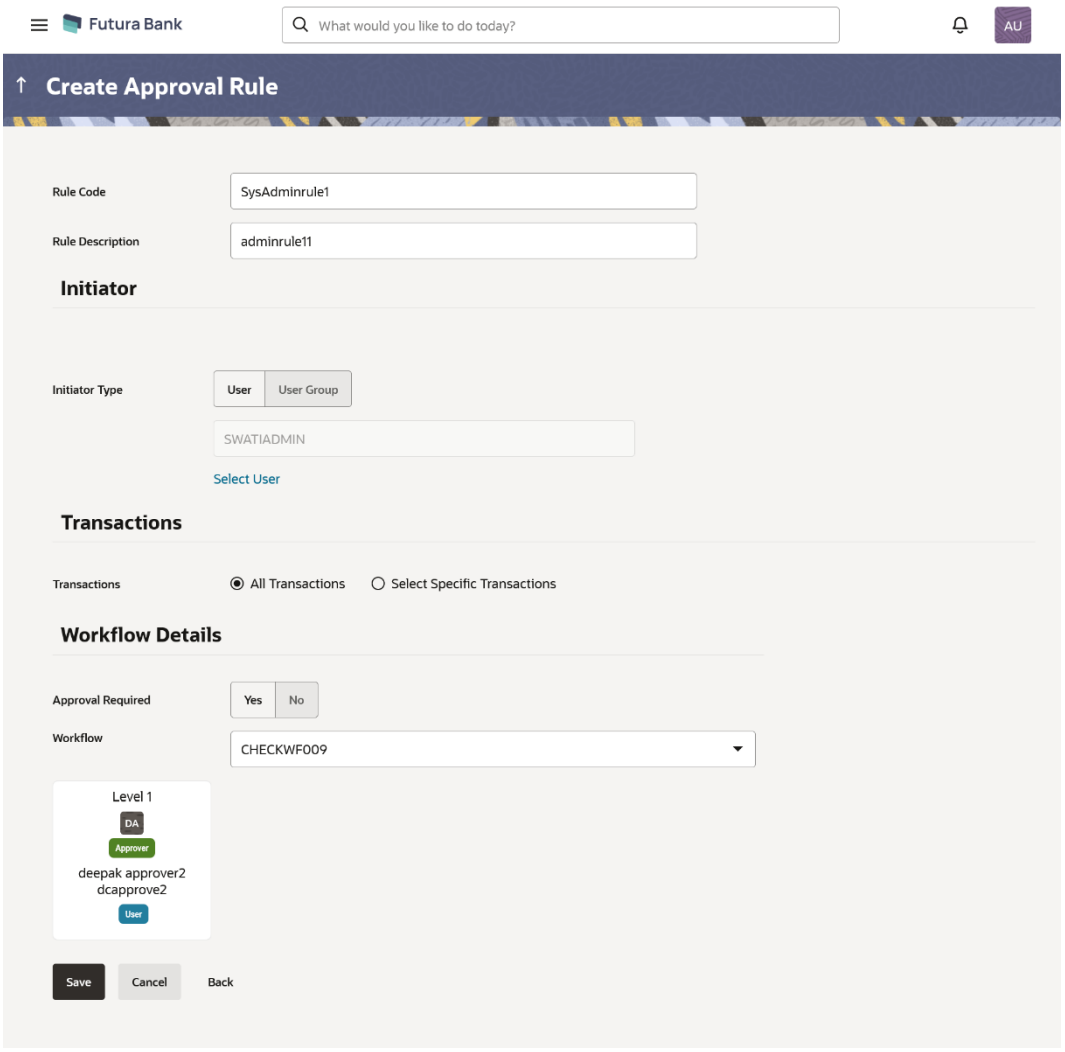
Bank Administrator can create multiple approval rules for Administrator users. In a scenario when a transaction is initiated and multiple rules are applicable as per set conditions, then the complex rule amongst all the applicable rules is applied for approval.

User can further define if for a condition, the transaction should be auto approved (which means there is no approval workflow and the transaction gets approved as soon as initiator submits the transaction) or should follow a set approval workflow and should get approved by the defined set of approvers. The same is achieved by attaching a workflow maintained for the administrator users.

To create an approval rule:

1. In the **Admin Approval Rules** screen, click **Create**. The **Admin Approval Rules - Create** screen appears.

Admin Approval Rules - Create



Field Description

Field Name	Description
Rule Code	To specify approval rule code.
Rule Description	To specify approval rule description.
Initiator	
Initiator Type	Initiator type who initiates the transaction. This has options as ‘User’ and ‘User Group’.
User Name / User Groups	Name of the user or user group as initiator. If initiator is selected as User, then all the users belongs to administrator user segment will be listed for selection. If initiator is selected as User Group, then all the user groups belongs to the administrator user segment will be listed for selection.
Transactions	All transactions to set the approval rules are listed. User can select specific transaction or all admin transactions.
Workflow Details	
Approval Required	Option to decide whether approval is required or not for the set condition.
Workflow	Field has description of the approval workflow. All workflows maintained for the administrator type of user segment are listed here along with the defined approval level for each of them. This field appears if you select **Yes** in the **Approval Required** field.

2. In the **Rule Code** field, enter the code.
3. In the **Rule Description** field, enter the rule name.
4. From the **Initiator Type** field, click appropriate user / user group and select the user/ user group.
5. From the **Transaction** list, select the transactions to be mapped to the rule.
6. In the **Workflow Details** section, select whether approval is required for the mapped transactions.
   a. If you select **Yes** option, select the appropriate **Workflow**.
7. Click **Save** to save the approval rule.
   OR
   Click **Cancel** to cancel the transactionOR
   Click **Back** to go back to previous screen.

8. The **Approval Rule - Create Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to go back to previous screen.
9. The success message of saving the created approval rule appears along with the transaction reference number and status.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

14.2.2.4 Admin Approval Rules - Edit

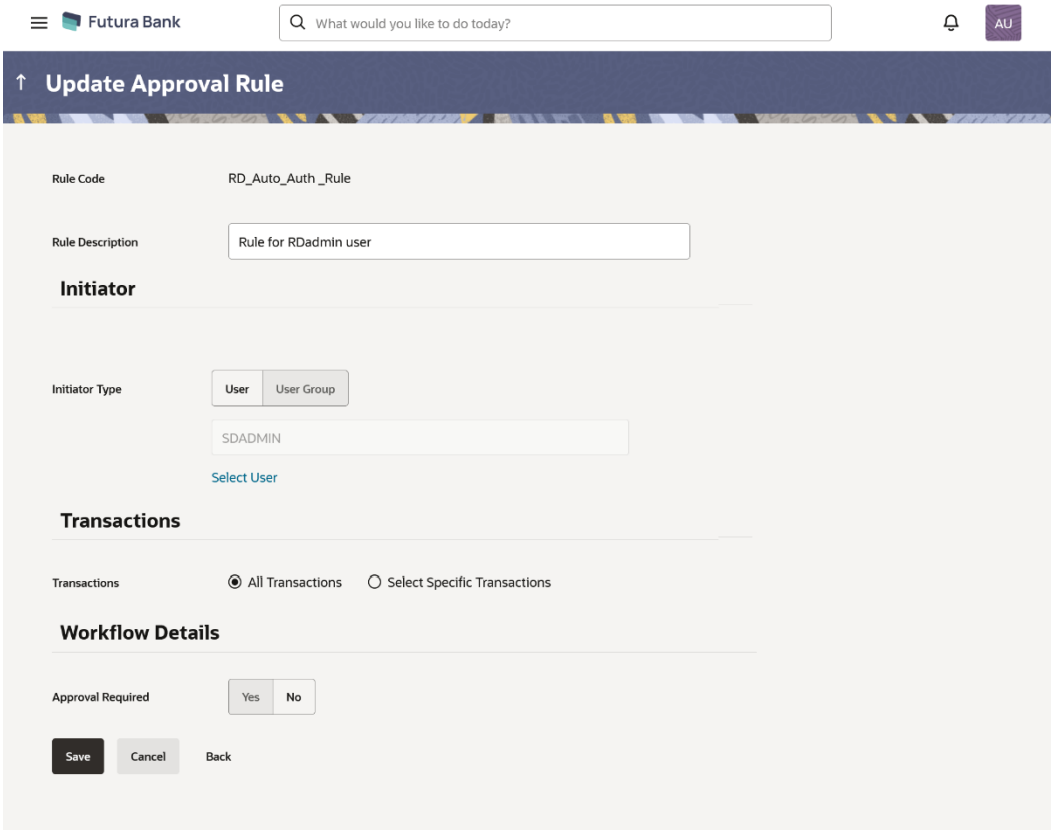
Bank Administrator can edit the approval rules. An Administrator is allowed to change the description of the rule and is also allowed to change the parameters associated with the specific approval rule.

Edited rules are applicable for new transactions initiated post rule update. Previously initiated transactions which are pending approval will follow a rule which was applied at the time of transaction initiation.

To edit an approval workflow:

1. In the **Admin Approval Rules** screen, click the **Rule Code** link, for which you want to view the details. The **Admin Approval Rules - View** screen appears.
2. Click **Edit**. The **Admin Approval Rules - Edit** screen appears.

Admin Approval Rules - Edit



Field Description

Field Name	Description
Edit	
Rule Code	Approval rule code provided by the user.
Rule Description	Approval rule description provided by the user in editable form.
Initiator	
Initiator Type	Initiator type who initiates the transaction will be displayed in editable form.

Field Name	Description
User Name / User Groups	Name of the user or user group as initiator will be displayed in editable form. If initiator is selected as User, then all the users belonging to the administrator type of user segment will be listed for selection. If initiator is selected as User Group, then all the user groups belonging to the administrator type of user segment will be listed for selection.
Workflow Details	
Approval Required	Whether approval is required will be displayed in editable form.
Workflow Details	Details of the approval workflow along with the defined approval levels for a condition will be displayed in editable form. This field appears if you select **Yes** in the **Approval Required** field.

3. Edit the required details.
4. Click **Save** to save the approval rule.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to cancel the operation and to go back to previous screen.
5. The **Admin Approval Rule - Edit Review** screen appears post necessary validations. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to go back to previous screen.
6. The success message of saving the approval rule modification appears along with the transaction reference number and status.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

14.2.3 Approval Rules - Retail & Business User - Approval Rule

This function will enable the Bank Administrator to set up conditions for approval as per the business requirements. A rule can be set up for financial, non-financial, and non-account financial transactions and for maintenance. Flexibility is provided to define approval rules with conditions stating that a 'specific transaction', if initiated by a 'specific user/ user group/All users', has to be approved by a 'specific approver/approver group' along with other attributes like amount range etc..

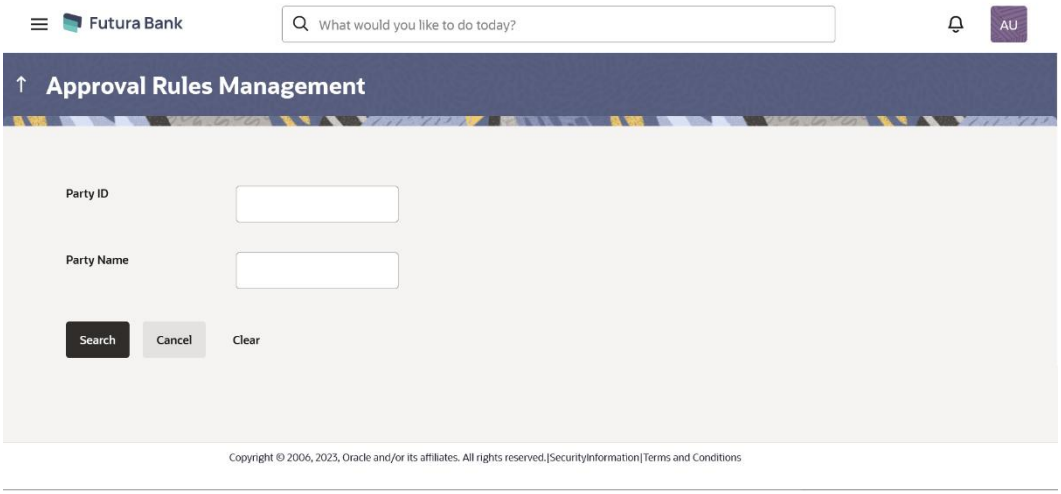
14.2.3.1 Approval Rules - Retail & Business User - Search

System displays a screen to enter the party ID or party name to search the approval rules that are maintained. User can enter the party ID (if known) or the party name with a minimum of 5 characters. System matches the input provided by the user with the party name records and displays the matching party records.

In case of a party search by party ID, it is an exact match and system displays the rules maintained if any.

In case of a party search by name, system displays the matching party records. The records have parties listed with both Party ID and Party Name information. User can select the record by clicking on the Party ID from the list.

Approval Rules - Retail & Business User



Field Description

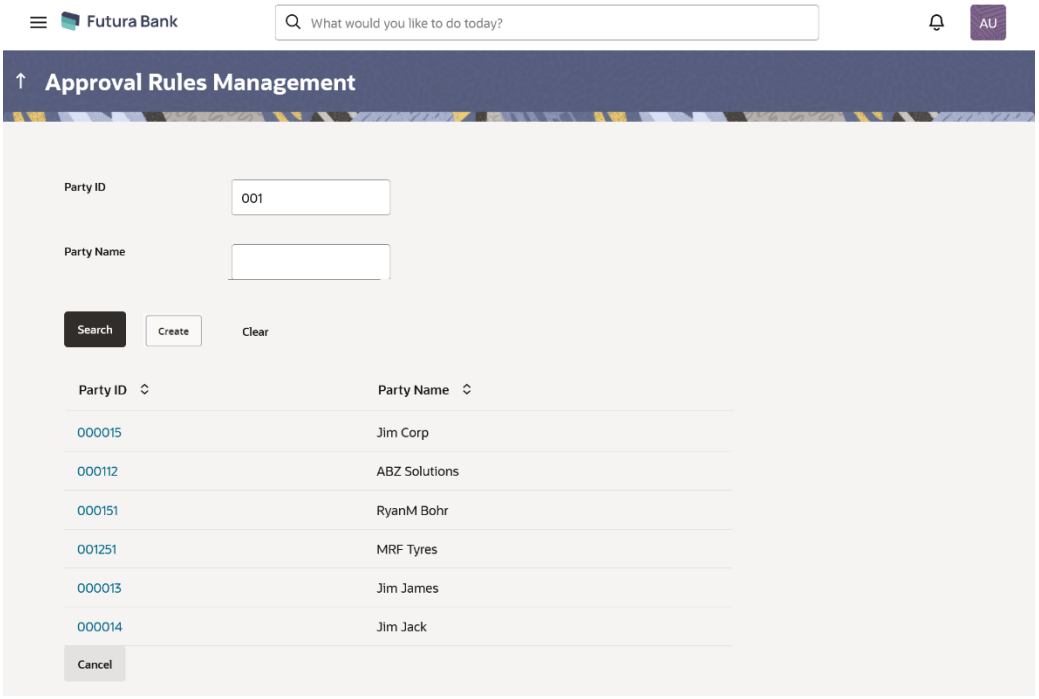
Field Name	Description
Party ID	Party ID as per search input.
Party Name	Party name of the party ID.

To search the approval rules for corporate users:

1. In the **Approval Rules** screen, enter the party ID in the In the **Party ID** field.
   OR
   In the **Party Name** field, enter the party name.
2. Click **Search** to search the matching records. The **Approval Rules** screen with search results appears based on the searched criteria.
   OR
   Click **Cancel** to cancel the operation and navigate the user back to 'Dashboard'.

OR
Click '**Clear**' to clear the input search parameters.

Approval Rules - Retail & Business User - Party Search

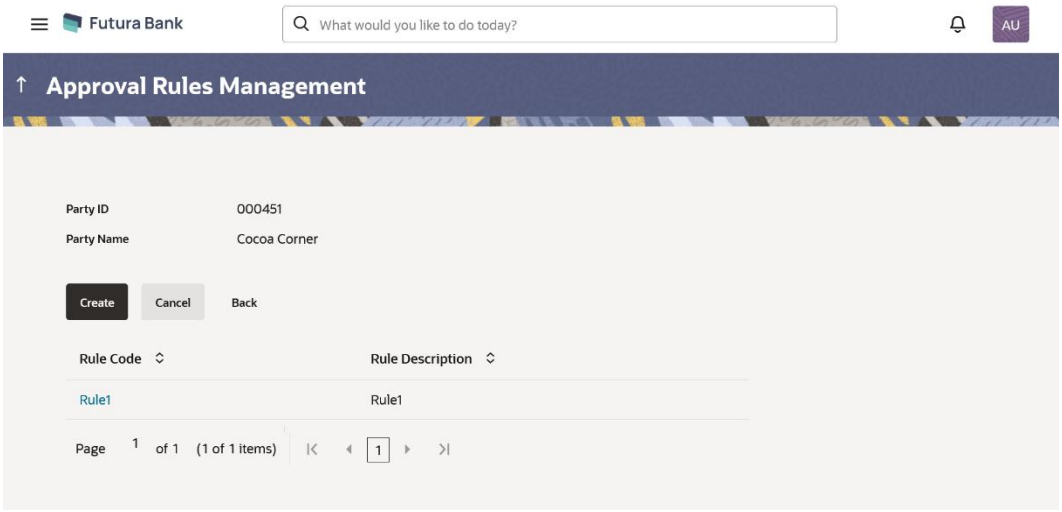


Field Description

Field Name	Description
Search Results	
Party ID	List of the Party ID as per search input.
Party Name	List of the Party names of the party IDs as per search input.

3. Click the **Party ID** link, to view details. The **Approval Rule - Summary** screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.

Approval Rule – Summary



4. Click the **Rule code** link, to view details of the selected Approval Rule. The **Approval Rules - View** screen appears.
   OR
   Click **Create** to create new Approval Rule for Retail & Business users.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to go back to previous screen.

14.2.3.2 Approval Rule – Retail & Business User - Create

Bank Administrator can create approval rules for the Retail & Business users. Administrator is allowed to create an approval rule only if the party preference is maintained and party is in active status.

Approval rules can be setup based on the following parameters.

- Type of Transaction
  - Financial Transactions
    - This option is used to setup approval rules for the transactions, this involves exchange of money.
    - E.g. Money Transfer, Draft Issuance, Redeem Term Deposit etc.
  - Non Financial Transactions
    - This option is used to setup approval rules for the transaction which are for an account, but does not involve exchange of money.
    - E.g. Cheque Book Request, Statement Request, Stop Cheque etc.
  - Maintenance
    - This option is used to setup approval rules for the transaction which are at the party level and not for a specific account
    - E.g. Payee Maintenance
  - Administration
    - Option is used to setup approval rules for the maintenances which corporate administrator can initiate. These are mainly configurations related transactions for that corporate
    - E.g. Account-Transaction mapping, Approval related maintenances etc.
  - Non Account Financial Transactions:
    - This option is used to setup approval rules for the transaction with amount range and no debit account
    - E.g. Initiate LC, Supply Chain Finance related transactions like create Invoice.
  - Initiator
    - Specific User
    - User Group
    - All Users
  - Accounts
  - Transactions
  - Currency
  - Amount Range

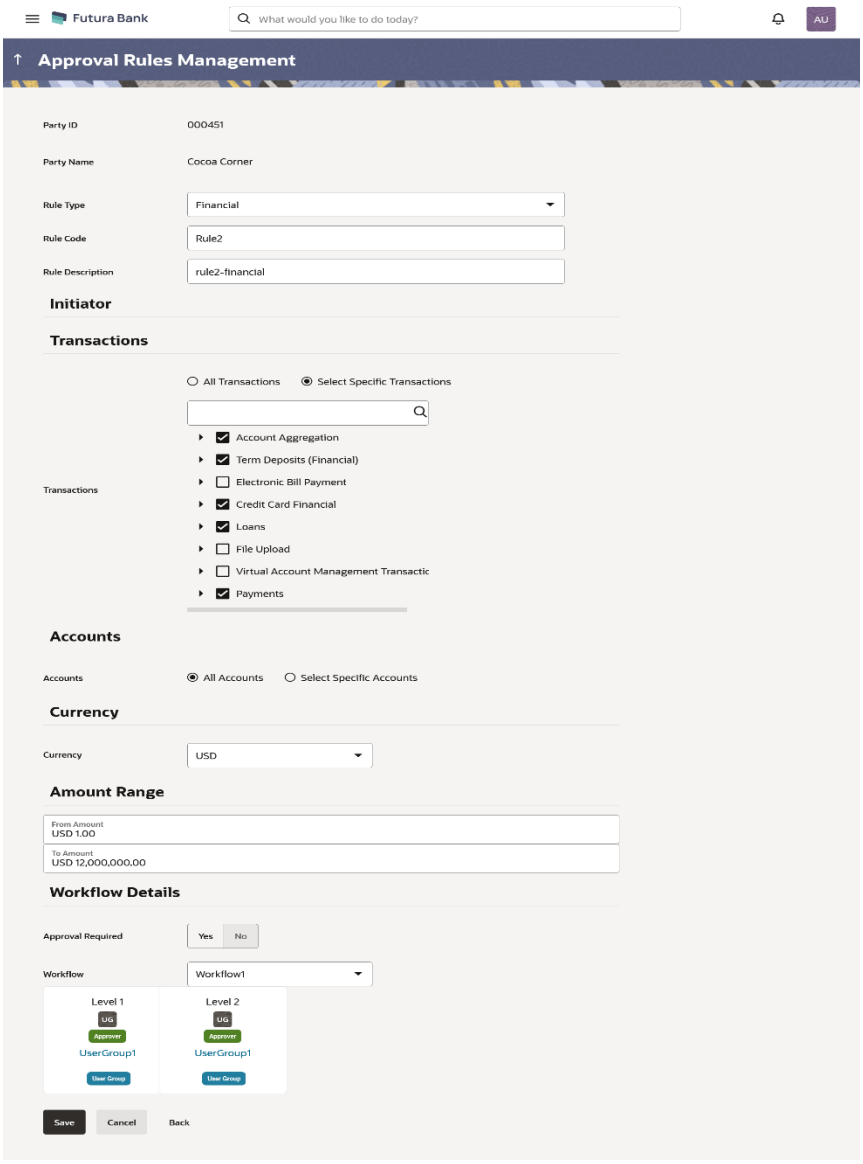
Administrator can create multiple approval rules for party users. In a scenario when a transaction is initiated and multiple rules are applicable as per set conditions, then the complex rule amongst all the applicable rules is applied for approval.

User can further define if for a condition, the transaction should be auto approved (which means there is no approval workflow and the transaction gets approved as soon as initiator submits the transaction) or should follow a set approval workflow and should get approved by the defined set of approvers. The same is achieved by attaching a workflow maintained for the Retail & Business party.

To create an approval rule for Retail & Business user:

1. In the **Approval Rules** screen, enter the search parameters and click **Search**. The **Approval Rules** screen with both Party ID and Party Name appears.
2. Click the **Party ID** link, to view details. The **Approval Rule - Summary** screen appears.
3. Click **Create**. The **Approval Rules - Create** screen appears.

Approval Rules – Retail & Business User - Create



Field Description

Field Name	Description
Party ID	Party ID for which an approval rule is to be maintained.
Party Name	Party name of Party ID for which an approval rule is to be maintained.
Rule Type	Transaction rule type for which the approval rule needs to be set up. The transaction rule for Retail & Business user are: • Financial • Non Financial • Maintenance • Administration • Non Account Financial The transaction rule types for a non-customer Retail & Business user are: • Maintenance • Non Account Financial • Administration
Rule Code	To specify approval rule code.
Rule Description	To specify approval rule description.
Initiator	
Initiator Type	Initiator type who initiates the transaction. This has options as ‘User’ , ‘User Group’ and ‘All Users’
User / User Group	Name of the user or user group as initiator. If initiator is selected as User, then all the users belongs to the party will be listed for selection. If initiator is selected as User Group, then all the user groups belongs to the party will be listed for selection. If Initiator is selected as ‘All Users’, then the rule which is being created is applicable for all users of Corporate Party.
Transactions	Type of transactions to set the approval rules. Type of transactions depends on the selection of rule type.

Field Name	Description
Accounts	Type of accounts. This field appears if you select **Financial** and **Non Financial** in the **Rule Type** field.
Currency	Currency type in which the financial approval rule for a corporate is defined. This field appears if you select **Financial** and **Non Account Financial** in the **Rule Type** field. Note: 1) Entity's base currency (maintained in system configuration) will be defaulted in the currency field. 2) User will be able to select the currency other than the default currency from the currency list.
Amount Range	
From Amount/ To Amount	Transactions allowed for the user between the amount range. This field appears if you select **Financial** and **Non Account Financial** in the **Rule Type** field.
Workflow Details	
Approval Required	Option to decide whether approval is required or not for the set condition.
Workflow	Field has description of the approval workflow. All workflows maintained for the party are listed here along with the defined approval level for each of them. This field appears if you select **Yes** in the **Approval Required** field.

4. In the **Rule Type** field, select the appropriate transaction rule type.
5. In the **Rule Code** field, enter the code.
6. In the **Rule Description** field, enter the rule name.
7. From the **Initiator Type** field, click appropriate user / user group and select the user/ user group or Select 'All Users'
8. From the **Transaction** list, select the transactions to be mapped to the rule.
9. From the **Accounts** list, select the appropriate account, if you have selected **Financial** option in the **Rule Type** field.
10. From the **Currency** list, select the appropriate account currency, if you have selected **Financial** option in the **Rule Type** field.

11. In the **Amount Range** section, enter the appropriate amount if you have selected **Financial** and **Non Account Financial** option in the **Rule Type** field.
12. In the **Workflow Details** section, select whether approval is required for the mapped transactions.
13. If you select **Yes** option, select the appropriate **Workflow**.
14. Click **Create** to save the approval rule.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
    OR
    Click **Back** to go back to previous screen.
15. The **Approval Rule - Create - Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the operation and navigate back to the 'Dashboard'.
    OR
    Click **Back** to go back to previous screen.
16. The success message of saving the created approval rule appears along with the transaction reference number and status.
    Click **OK** to complete the transaction and navigate back to 'Dashboard'.

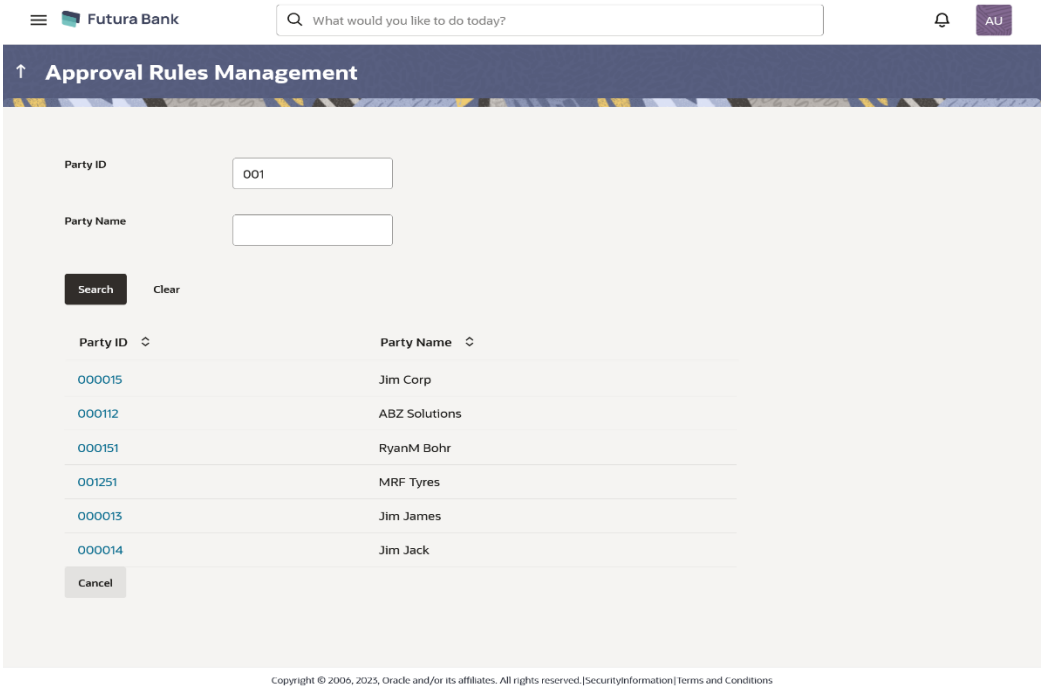
14.2.3.3 Approval Rules – Retail & Business User – Rule Summary

Bank Administrator logs into the system and navigates to the Rules Management screen, and searches the party. On accessing the party ID, approval rules maintained (if any) for the party mapped to the user are displayed on the screen. User can opt to view the details of existing rules or can create new approval rule using this screen.

How to reach here:

Dashboard > Toggle Menu > Approvals > Rule Management > Retail & Business User > Search Party > View Rule summary

Approval Rule – Search

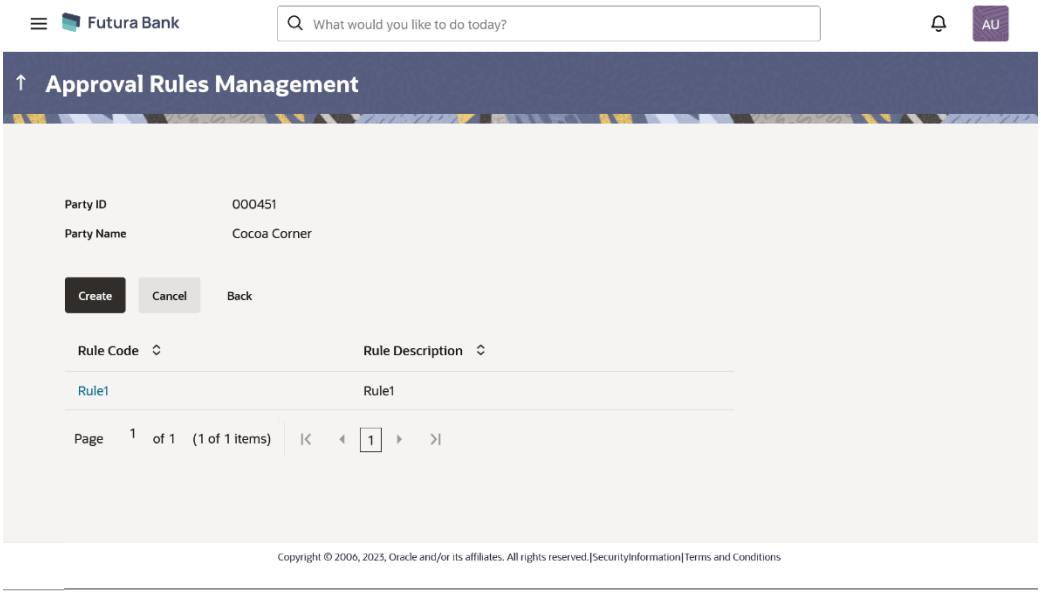


Field Description

Field Name	Description
Party ID	Party ID for which an approval rule is to be viewed.
Party Name	Party name of Party ID for which an approval rule is to be viewed.
Search Results	
Party ID	List of the Party IDs as per search input.
Party Name	List of the Party names of the party IDs as per search input.

1. Click the **Party ID** link to view details. The Approval Rule - Summary screen appears.

Approval Rule – Summary



Field Description

Field Name	Description
Party ID	Party ID for which an approval rule is to be viewed.
Party Name	Party name of Party ID for which an approval rule is to be viewed.
Search Results	
Rule Code	The approval rule code.
Maker	Initiator type (User ID or User Group Code) of the transaction. This field will be displayed only if existing approval rules are available under a party.
Approval Required	Whether approval is required for each rule maintained.
Workflow Code	The approval workflow code.

2. Click the **Rule code** link, to view details of the selected Approval Rule. The **Approval Rules - View** screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to go back to previous screen.

OR
Click **Create** to create new Approval Rule for corporate users.

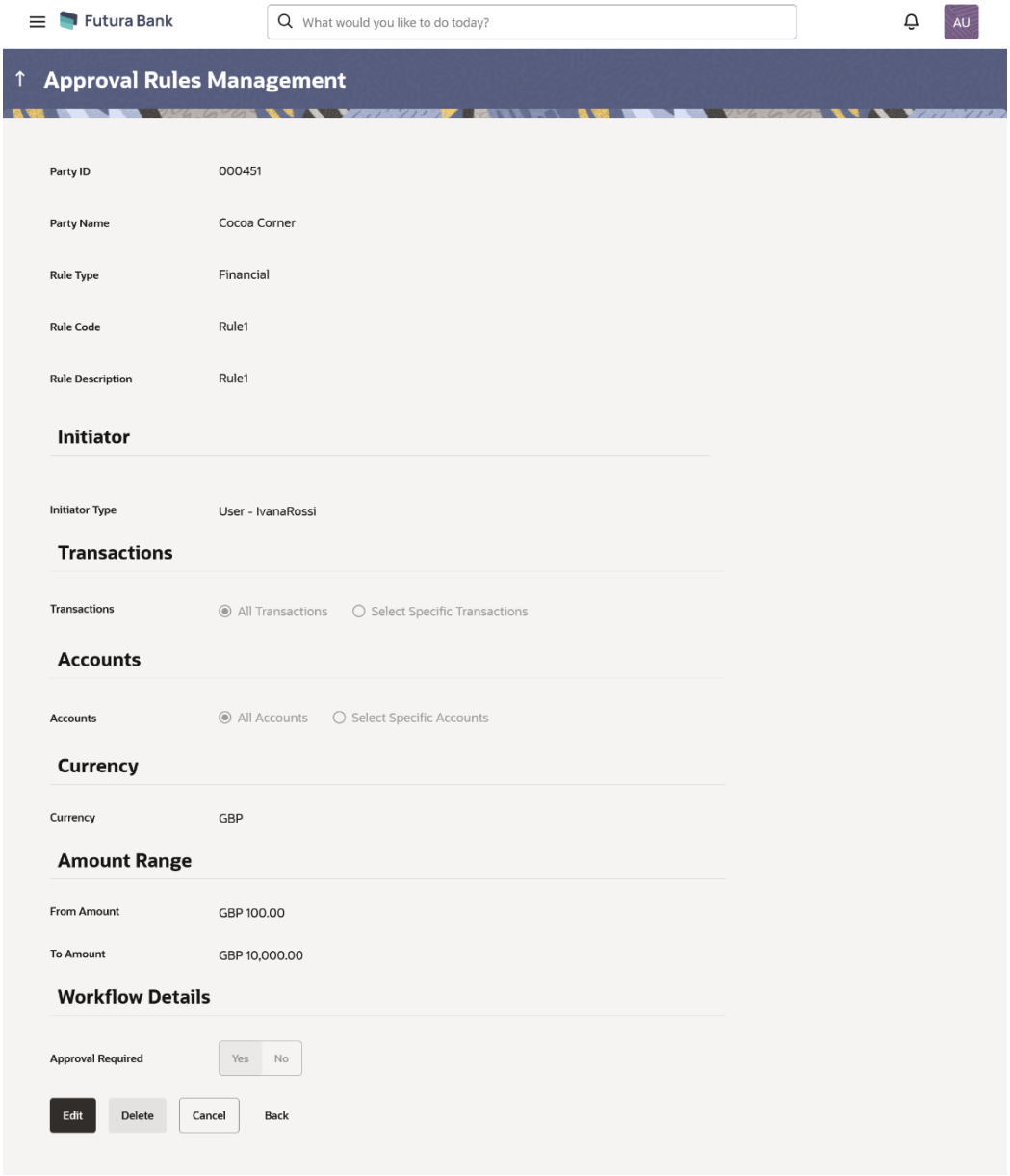
14.2.3.4 Approval Rules - Retail & Business User- View

On accessing 'Rules Management' menu option, and searching rules by providing party ID, summarized view of all the approval rules maintained (if any) for the party are displayed on the screen. Further drill down is given on the each rule to view the details of approval rule.

To view the approval rules for Retail & Business users:

1. In the **Approval Rules** screen, enter the search parameters and click **Search**. The **Approval Rules** screen with both Party ID and Party Name appears.
2. Click the **Party ID** link, to view details. The **Approval Rule - Summary** screen appears.
3. Click the **Rule Code** link, for which you want to view the details. The **Approval Rules - View** screen appears.

Approval Rules View



Field Description

Field Name	Description
View	
Party ID	Party ID for which an approval rule is to be viewed.

Field Name	Description
Party Name	Party name of Party ID for which an approval rule is to be viewed.
Rule Type	Transaction rule type for which the approval rule is set up. The transaction rule for Retail & Business user are: • Financial • Non-Financial • Maintenance • Administration • Non Account Financial The transaction rule types for a non-customer Retail & Business user are: • Maintenance • Non Account Financial • Administration
Rule Code	Approval rule code.
Rule Description	Approval rule description.
Initiator	
Initiator Type	Initiator type specified while creating a rule. Note : “ All Users’ will be displayed for Initiator Type if rule is created with Initiator type as “All users”
User Name / User Groups	Name of the user or user group defined as initiator for the rule condition.
Transactions	Transaction for which the rule is set up.
Accounts	Field will display the account for which rule being viewed is set up. This field appears if you select **Financial** and **Non Financial** in the **Rule Type** field.

Field Name	Description
Currency	Currency type in which the financial approval rule for a corporate is defined. This field appears if you select **Financial** and **Non Account Financial** in the **Rule Type** field. Note: 1) Entity's base currency (maintained in System Configuration) will be defaulted in the currency field. 2) User will be able to select the currency other than the default currency from the currency list.
Amount Range	
From Amount/ To Amount	Transactions allowed for the user between the amount range. This field appears if you select **Financial** and **Non Account Financial** in the **Rule Type** field.
Workflow Details	
Approval Required	Field displays whether approval is required or not.
Workflow Details	Field displays the approval workflow details along with the defined approval levels. This field appears if you select **Yes** in the **Approval Required** field.

4. Click **Edit** to edit the approval rule. The **Approval Rule - Edit** screen with values in editable form appears.
   OR
   Click **Delete** to delete the approval rule.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to previous screen.
   The application will prompt the administrator with a deletion message, Click **Yes** to confirm.
   User is directed to **Admin Approval Rule – Delete** confirmation page.

14.2.3.5 Approval Rules - Retail & Business User- Edit

Bank Administrator can edit the approval rules. An administrator is allowed to change the description of the rule and is also allowed to change the parameters associated with the specific approval rule.

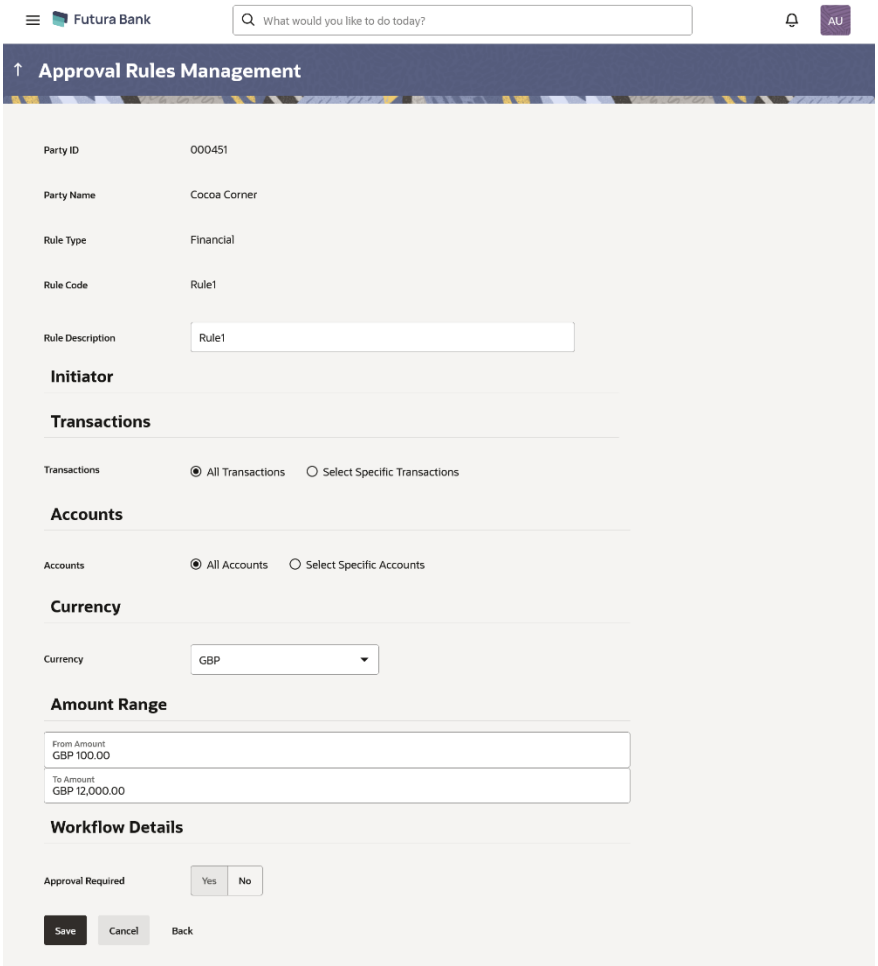
Modifications in approval rule are allowed only if the party preference is in active status.

Edited rules are applicable for new transactions initiated post rule update. Previously initiated transactions which are pending approval will follow a rule which was applied at the time of transaction initiation.

To edit an approval rule:

1. In the **Approval Rules Management** screen, enter the search parameters and click **Search**. The **Approval Rules** screen with both Party ID and Party Name appears.
2. Click the **Party ID** link, to view details. The **Approval Rule - Summary** screen appears.
3. Click the **Rule Code** link, for which you want to view the details. The **Approval Rules - View** screen appears.
4. Click **Edit** to edit the approval rule. The **Approval Rule - Edit** screen with values in editable form appears.

Approval Rules - Edit



Field Description

Field Name	Description
Edit	
Party ID	Party ID for which an approval rule is to be modified.
Party Name	Party name of Party ID for which an approval rule is to be modified.
Rule Type	Transaction rule type for which the approval rule is set up will be displayed. The transaction rule for corporate user are: • Financial • Non Financial • Maintenance • Administration • Non Account Financial The transaction rule types for a non-customer corporate user are: • Maintenance • Non Account Financial • Administration
Rule Code	Approval rule code provided by the user.
Rule Description	Approval rule description provided by the user in editable form.
Initiator	
Initiator Type	Initiator type who initiates the transaction will be displayed in editable form. Note : Select 'All Users' if rule is being created is applicable for all users of Corporate Party
User Name / User Groups	Name of the user or user group as initiator will be displayed in editable form. If initiator is selected as User, then all the users belonging to the party will be listed for selection. If initiator is selected as User Group, then all the user groups belonging to the party will be listed for selection.

Field Name	Description
Transactions	Type of transactions to set the approval rules will be displayed in editable form. Type of transactions depends on the selection of rule type.
Accounts	Type of accounts will be displayed in editable form. This field appears if you select **Financial** and **Non Financial** in the **Rule Type** field.
Currency	Currency type in which the financial approval rule for a corporate is defined.
Amount Range	
From Amount/ To Amount	Transactions allowed for the user between the defined amounts ranges will be displayed in editable form. This field appears if you select **Financial and Non Account Financial** in the **Rule Type** field.
Workflow Details	
Approval Required	Whether approval is required will be displayed in editable form.
Workflow Details	Details of the approval workflow along with the defined approval levels for a condition will be displayed in editable form. This field appears if you select **Yes** in the **Approval Required** field.

5. Edit the required details.
6. Click **Save** to save the approval rule.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to cancel the operation and to go back to previous screen.
7. The **Approval Rule - Edit Review** screen appears post necessary validations. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'
   OR
   Click **Back** to cancel the operation and to go back to previous screen.
8. The success message of saving the approval rule modification appears along with the transaction reference number and status.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

FAQ

1. **How many approval levels can I set up in the system?**

   Administrator can set up minimum one and maximum five levels of approvals as a part of approval workflow. Whereas, maximum levels of approvals that the user can set is configurable as Day0.

2. **Which approval rule will get applied when multiple applicable approval rules are found for specific transaction?**

   In a scenario when a transaction is initiated and multiple rules are applicable as per set conditions, then the complex rule amongst all the applicable rules is applied for approval.

3. **What happens to the approval process when approval rule gets edited and a transaction is pending with one of the approver for approval?**

   Edited rules are applicable for new transactions initiated post rule update. Previously initiated transactions which are pending for approval will follow a rule which was applied at the time of transaction initiation.

4. **What happens if the transaction is initiated in the currency in which approval rule is not maintained?**

   If the rule is not maintained in specific currency, then the approval rule set in the local currency for the transaction and amount combination will be applied.

5. **What happens if the approval rule in local currency is not maintained in above scenario?**

   If the approval rule is not set for both transaction currency and local currency, then transaction cannot be initiated.

15. Group Corporate Onboarding

Corporate onboarding is the process that bank undertakes when bringing a new business customer onboard. OBDX furnishes integrating the onboarding workflow to a business rules engine that facilitates uninterrupted corporate onboarding processing. Generally, the customer onboarding process constitutes of multiple activities.

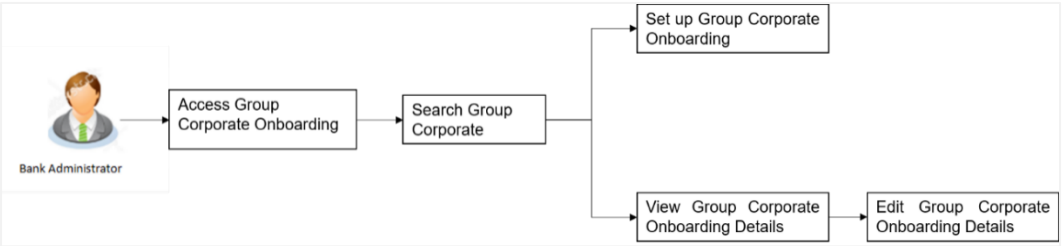
Group corporate onboarding allows the administrator to onboard the corporate party on OBDX along with definition of various attributes including Group Corporate Profiling, Party and User Account Access, User Onboarding, User Group Maintenance, User Reports Mapping, Approvals Workflow and Rules Maintenance etc. in a single flow. After performing these onboarding steps in a single flow, the applications send the same as a single approval.Group corporate onboarding allows corporate parties belonging to different entities to map under a Group Corporate ID.

Group Corporate onboarding function would be a two-step process. Bank admin would be required to onboard Corporate using his party ID and then proceed to Group Corporate Onboarding wizard.

This maintenance is done only for corporate type of parties and is not applicable for retail & business type of parties. Parameter values maintained against a Group Corporate defines the system behavior for the following:

- Accessible Roles for Group Corporate
- Workflow and Approval Flow preference
- Party and User level account access
- User onboarding with multi-entity setup and accessible Party Maintenance
- User Group Maintenance for Group Corporate users
- Corporate user report mapping maintenance to generate user reports
- Approval workflow and Rules setup for banking transaction

Workflow



Features supported in the Application

- Setup Group Corporate Onboarding
  - Group Corporate Profiling
  - Party Account Access
  - User Onboarding
  - User Group Maintenance
  - User Account Access
  - User Reports Mapping
  - Approval –Workflow Management
  - Approval – Rules Management
- View Group Corporate Onboarding Details
- Edit Group Corporate Onboarding Details

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Corporate Onboarding > Group Corporate *Onboarding*
OR
System/ Bank Administrator Dashboard > Corporate Onboarding > Group Corporate Maintenance

15.1 Group Corporate Onboarding – Search Corporate

Bank administrator logs in to the application and navigates to the Group Corporate onboarding Screen. On this screen, the administrator will be required to search a Group Corporate and select the required Group Corporate name from the search results, for setting up the onboarding functions.

System allows bank admin to search Group Corporate by using either Group Corporate details or Corporate Party details.

To search using Group Corporate details, application gives a provision to enter the Group Corporate information including Group Corporate ID and Group Corporate Name.

User can enter the Group Corporate ID (if known) or the Group Corporate name with a minimum of 1 characters. System matches the input provided by the user with the Group Corporate name records and displays the matching group corporate records.

User can enter party information including Entity ID, Party ID or Party Name, if searching the Group Corporate using Party details.

User can enter the Entity ID, Party ID (if known) or the Party Name with a minimum of 5 characters. System matches the input provided by the user with the Party Name records and displays the matching group corporate details.

To search Group Corporate (Using Group Corporate Details):

1. In the **Search By** field, select the appropriate option to search the Group Corporate.

   b. If you select the **Group Corporate** option;

      i. In the **Group Corporate ID** field, enter the Group Corporate ID whose Group Corporate Details you wish to view.
      OR
      In the **Group Corporate Name** field, enter the name of the Group Corporate whose Group Corporate Details you want to view.

   c. If you select the **Party** option;

      ii. In the **Party ID** field, enter the party ID mapped to Group Corporate you wish to view. The **Search Party** popup appears.

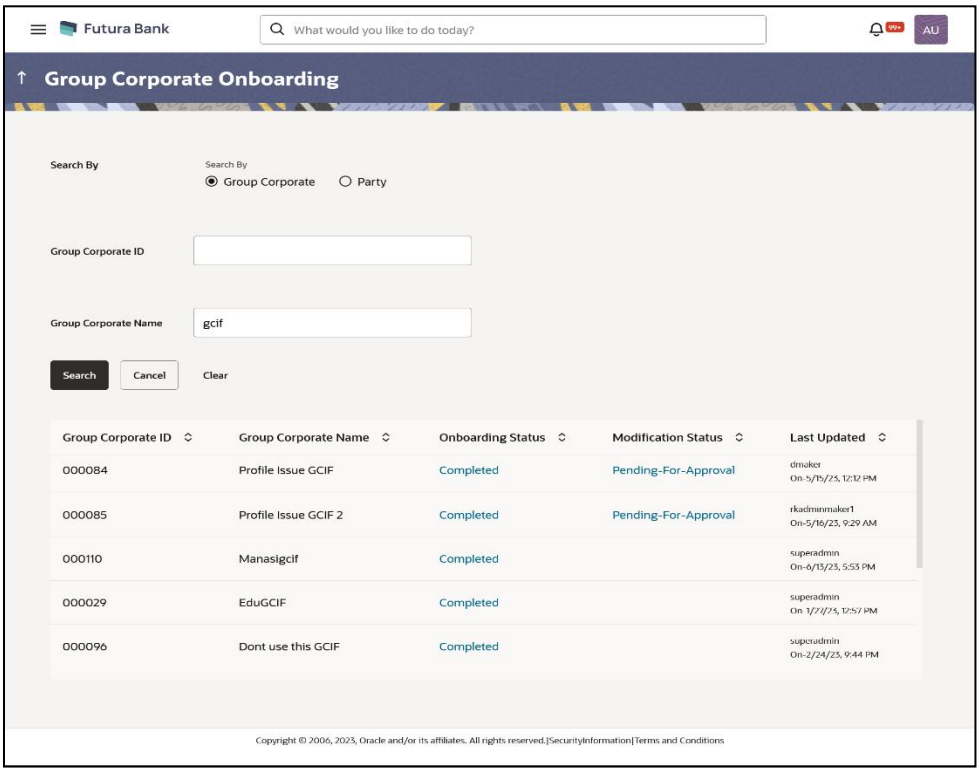
      iii. From the **Entity ID** list, select the entity from which party to be searched.

      iv. In the **Party ID** field, enter the party ID to be searched.
      OR
      In the **Party Name** field, enter the name of the party to be searched.

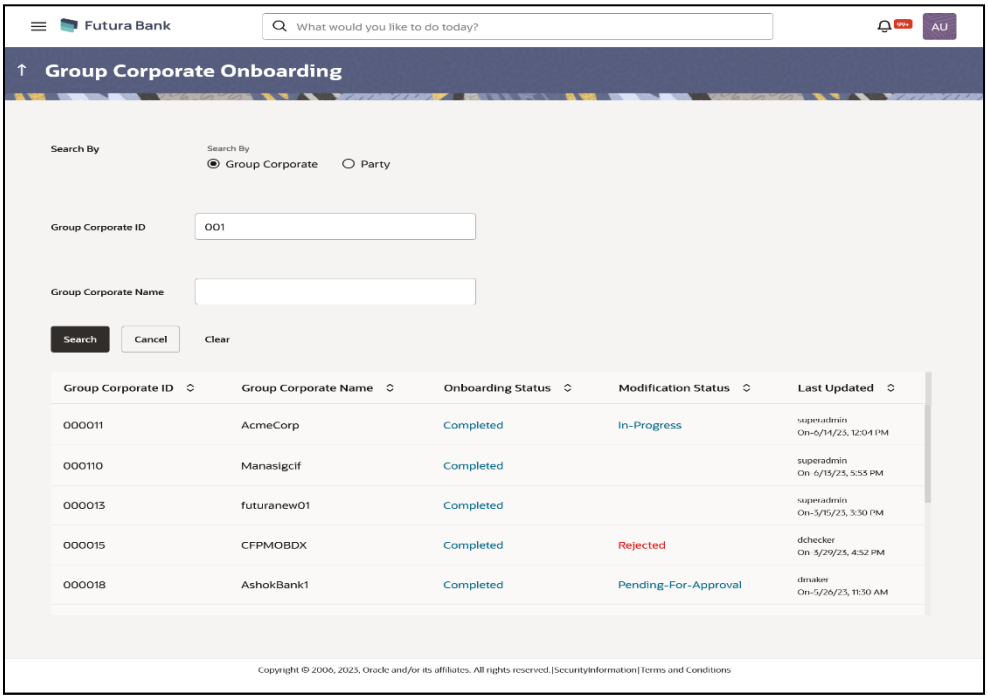
      v. Click **Search** to search the party mapped to the Group Corporate.
      OR
      Click **Cancel** to cancel the transaction
      OR
      Click **Clear** to reset the entered details.

2. Click **Search**.
   The Group Corporate summary screen appears with search results as per the searched criteria.
   In case of invalid Group Corporate details, appropriate error message is shown on the screen.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.

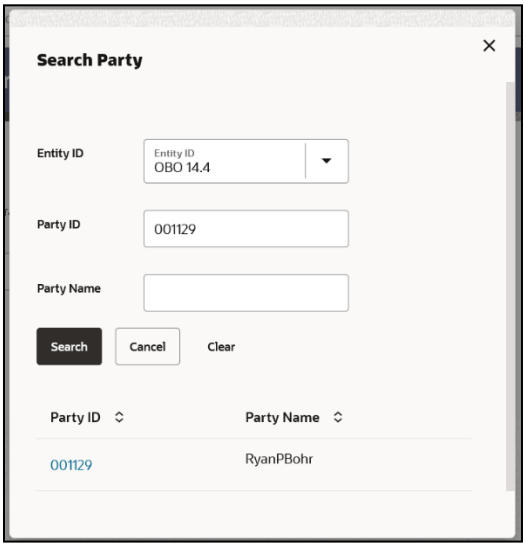
Group Corporate – Search by Group Corporate Name



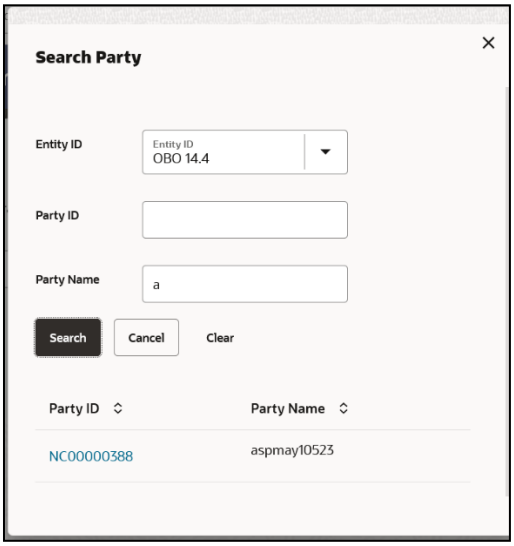
Group Corporate – Search by Group Corporate ID



Group Corporate – Search by Party ID



Group Corporate – Search by Party Name



Format Description

Field Name	Description
Search By Group Corporate Details	
Group Corporate ID	Group Corporate ID for which Group Corporate onboarding is to be maintained/ viewed.

Field Name	Description
Group Corporate Name	Group Corporate Name for which Group Corporate onboarding is to be maintained/ viewed.
Search By Corporate Party Details	
Entity ID	Entity ID of the Corporate Party
Party ID	Party ID for which Group Corporate onboarding is to be maintained/ viewed.
Party Name	Party Name for which Group Corporate onboarding is to be maintained/ viewed.
Search Results	
Group Corporate ID	Group Corporate ID for which Group Corporate onboarding is to be maintained/ viewed.
Group Corporate Name	Group Corporate ID for which Group Corporate onboarding is to be maintained/ viewed.
Onboarding Status	Onboarding status of Group Corporate in Application
Modification Status	Modification status of Group Corporate in Application
Last Updated	Last updated details for the Group Corporate.

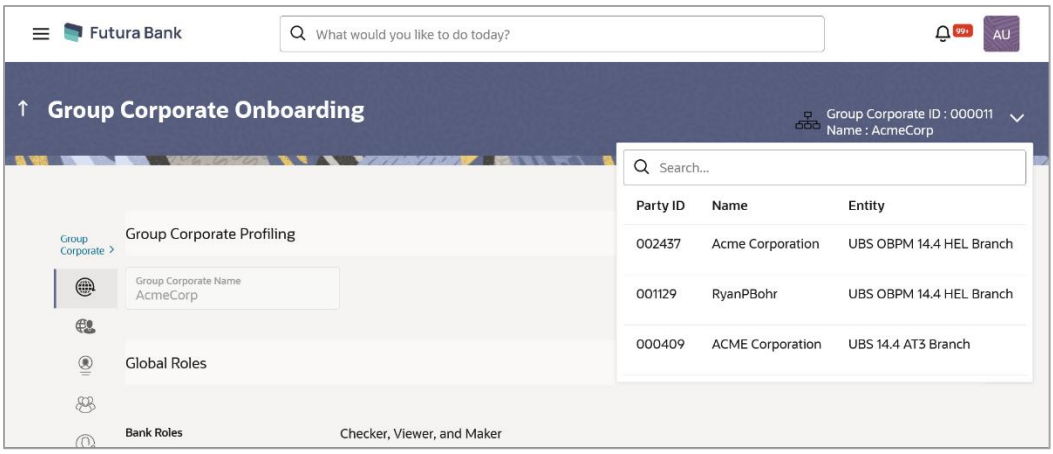
3. Click the **Onboarding Status** link, to view details of the selected Group Corporate. The **Group Corporate - View** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the input search preference.

15.1.1 View Linked Parties under Group Corporate

The Bank Administrator can view the linked parties under the selected Group Corporate on the Group Corporate Onboarding screen on expanding the Group Corporate details on right top corner. **To search linked parties under Group Corporate:**

1. Click on icon adjacent to the Group Corporate ID. An expansion is visible on the Group Corporate ID from where the user can view the list of parties mapped to the Group Corporate along with the ID, name and entity details of each mapped party.

Note: A specific party can be searched by providing the Party ID, Name or Entity in the search field.



Field Description

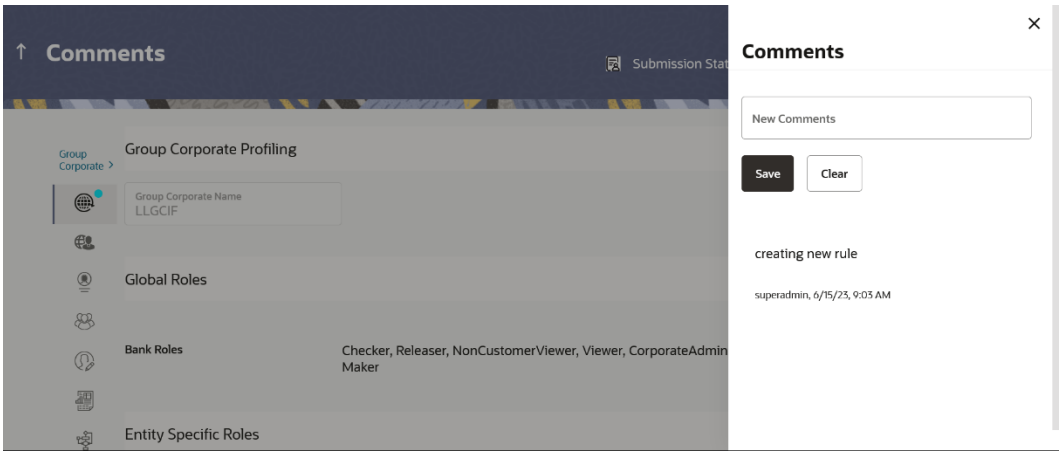
Field Name	Description
Search	Allows user to search for the specific Party by giving the ID, Name or Entity
Party ID	Displays Party ID of the existing linked party for respective group corporate ID/ Name
Name	Displays Party Name of the existing linked party for respective group corporate ID/ Name
Entity	Displays Entity of the existing linked party for respective group corporate ID/ Name

15.1.2 Comments

Click on Comments icon to view / add stage wise comments. These comments can be added by any user involved in the maintenance journey e.g., maker, checker etc.

Note:
• The comments can be captured at each resource level.
• Multiple comments can be captured for one resource.
• The user ID and date timestamp will be available for each comment.
• The user can add comments however the added comments cannot be modified or deleted.
• The comments will be available in the activity log for the Group Corporate against the transaction reference number as long as the Group Corporate data is not purged.
• A history of comments will be available in case the maintenance is picked up by another approver of same user group for action. The reference number of the transaction continues to be the same and hence the comments trail can be viewed.

Comments Capture



1. Enter the comments.
2. Click **Save** to save the comments.
   OR
   Click **Clear** to reset the data entered.

15.1.3 Ready to Submit

Any user who modifies a resource in the entire Group Corporate maintenance is registered in the system as a contributor. When any user submits a transaction, a check is performed if all the contributors have given readiness for submission or not.

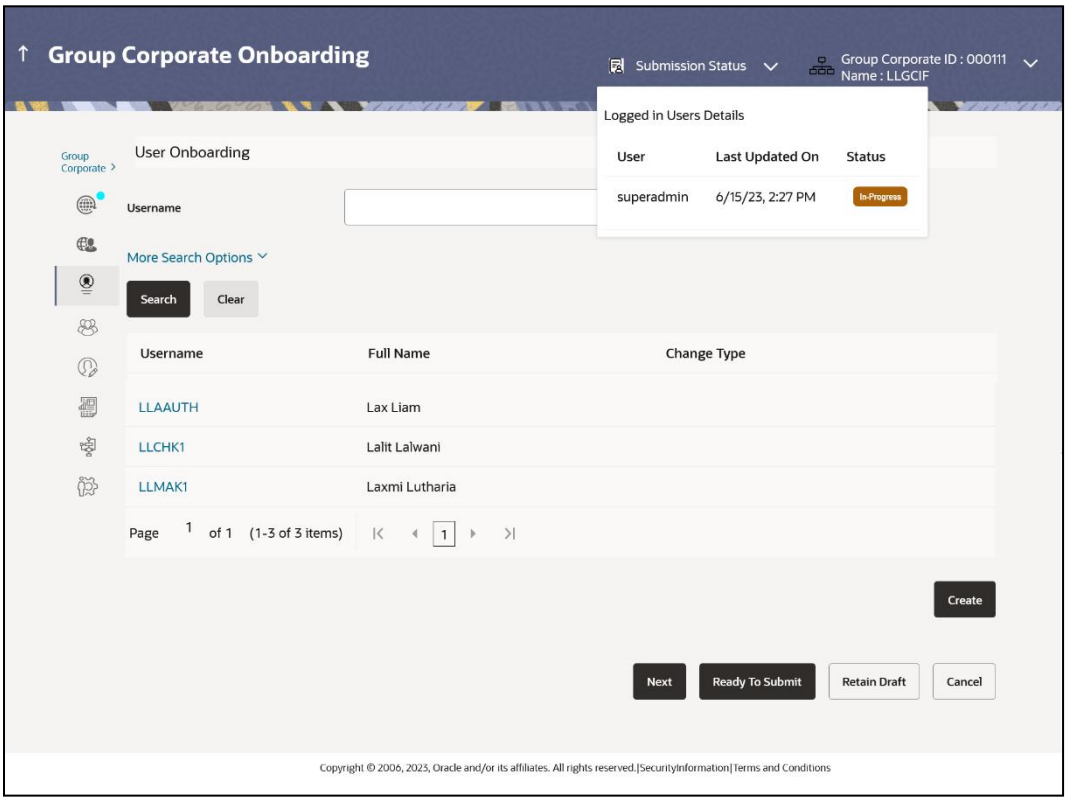
When any user submits a transaction, a check is performed and if all contributors have given readiness, then the transaction gets submitted successfully.

Note: Any user who has not performed any data modification on any step in the Group Corporate onboarding wizard but has only entered comments for a resource will not be considered as a contributor.

3. Update the transaction details and click **Save**.
4. On the **Group Corporate Onboarding** screen on top right corner, click on icon adjacent to **Submission Status**. Displays the status of the transaction submission readiness.

Note: The status of the transaction is **In-progress** until the user provides readiness for submission.

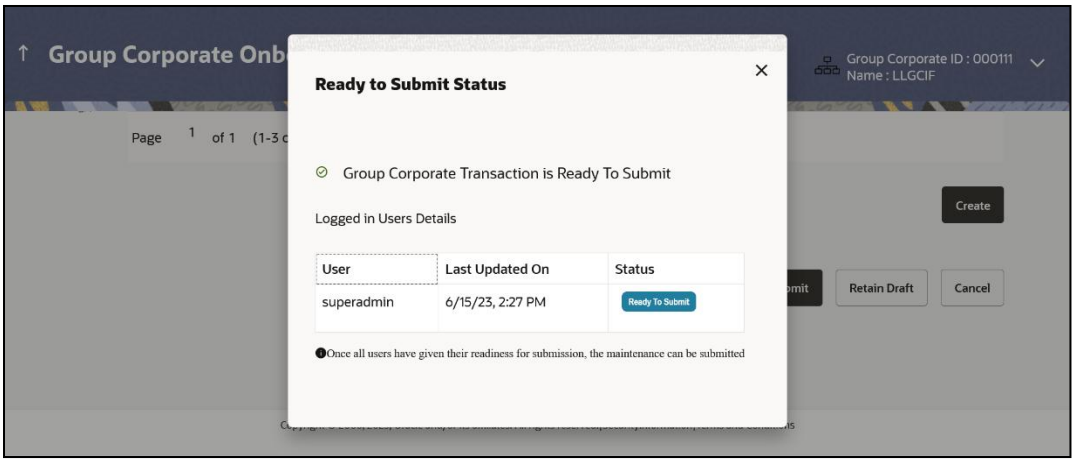
Modified Transaction with status



5. Click **Ready to Submit**. The **Ready to Submit Status** modal window appears.

Note: The status of the transaction changes to **Ready to Submit**.

Ready to Submit Status modal window



6. A check is performed and after all contributors have given readiness, the transaction is submitted successfully.

Note: The first user to submit changes will be the initiator, so their rule will be applicable. By default the field is disabled.

15.2 Step 1: Group Corporate Profiling

Group Corporate Profiling will allow the bank administrator to maintain Group Corporate Profiling considering various aspect.

While setting up the Profiling, bank administrator can define the accessible roles at Group corporate level. System will display all the roles available at enterprise level (Application roles are created using Role Transaction Mapping screen).

Administrator can enable corporate administration facility to handle various administrative maintenance on behalf of the Group Corporate . Such delegated users with an administrator role will have restricted scope over these administration functionalities and manage the Group Corporate to which they belong.

Administrator can select and assign the roles available at enterprise level as is, or user can create a custom role for the Group Corporate by cloning a role available at Group Corporate level. If Administrator creates a custom role for the Group Corporate by cloning a bank role, user can make the changes in that role on the overlay and save it with a different name. Admin will be able to remove touch points, modules, transactions, actions at the time of modifying the role (on the overlay).

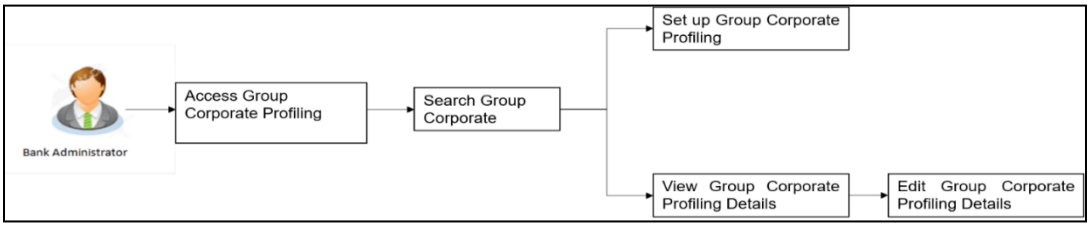
User can define the Approval workflow type, if it has to be sequential or parallel.

The admin can also specify whether release facility is enabled at the Group Corporate level or not.

Pre-Requisites

- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.
- Party for which Group corporate needs to be set up is created in core banking application

Workflow



How to reach here:

System/ Bank Administrator Dashboard > Corporate Onboarding > Group Corporate Onboarding > Group Corporate Profiling
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Group Corporate Onboarding > > Group Corporate Profiling

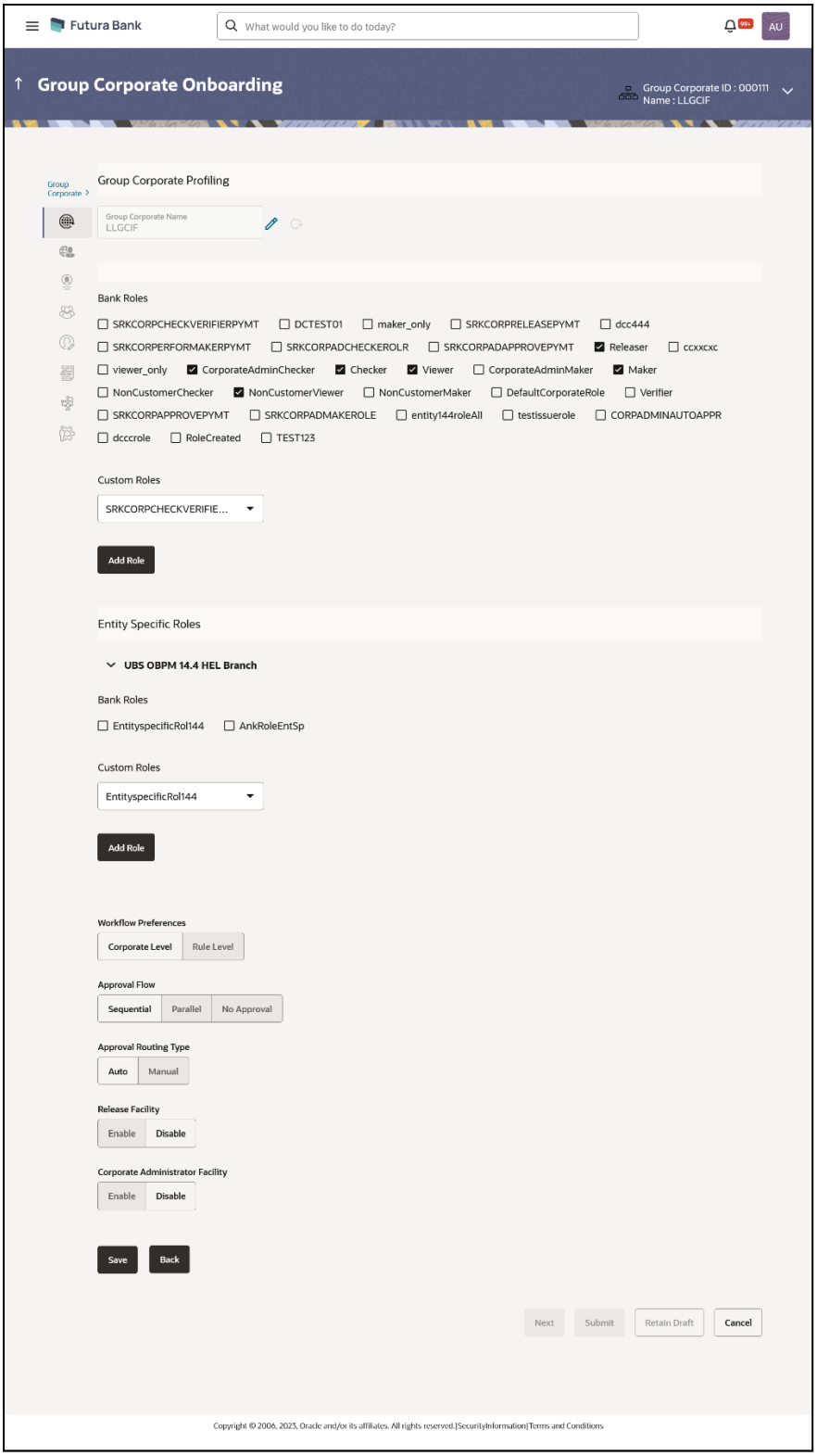
15.2.1 Group Corporate Profiling - Create

Using this option, Bank Administrator can configure Group Corporate Profiling for a specific Group Corporate ID.

To setup a Group Corporate Profiling:

1. In the **Search By** field, select the appropriate option to search the Group Corporate.
   a. If you select the **Group Corporate** option;
      i. In the **Group Corporate ID** field, enter the Group Corporate ID whose Group Corporate Details you wish to view.
      OR
      In the **Group Corporate Name** field, enter the name of the Group Corporate whose Group Corporate Details you want to view.
   b. If you select the **Party** option;
      i. In the **Party ID** field, enter the party ID mapped to Group Corporate you wish to view. The **Search Party** popup appears.
      ii. From the **Entity ID** list, select the entity from which party to be searched.
      iii. In the **Party ID** field, enter the party ID to be searched.
      OR
      In the **Party Name** field, enter the name of the party to be searched.
      iv. Click **Search** to search the party mapped to the Group Corporate.
      OR
      Click **Cancel** to cancel the transaction
      OR
      Click **Clear** to rest the entered details.
2. Click **Search**.
   The Group Corporate summary screen appears with search results as per the searched criteria.
3. Select **Group Corporate ID** from Group Corporate summary details.

Group Corporate Profiling – Create



Field Description

Field Name	Description
Group Corporate Name	Name of the group corporate.
Global Role	
Bank Roles	Display all the roles available at enterprise level.
Entity Specific Roles	The roles associated with different entities .
Customer Role	Create a custom role for the Group Corporate by cloning a role available at Group Corporate level. **Note** : Admin will be able to assign a mix of bank roles and custom roles to a Group Corporate
Workflow Preferences	The preference to implement the workflow. Possible value will be: • Corporate Level • Rule Level
Approval Flow	Define the Approval workflow type. Possible value will be: • Sequential • Parallel • No Approval This field is enabled if **Corporate Level** option is selected in **Workflow Preferences** field.

Field Name	Description
Approval Routing Type	Define the approval routing type. Possible value will be: • Auto- System will resolve the rule and the transaction will be sent for approval as per the rule resolved by the system. A rule which is having amount slab closest to the transaction amount will be resolved. The user will not have an option to select the approval workflow if routing type is Auto • Manual- User will be able to select a workflow from the resolved rules as part of transaction initiation Note: In case system resolves multiple rules with different min-max slabs, then as per rule resolution logic, it will resolve the rule which has the nearest 'max' value in the defined slab. 1) A Day 0 configuration is provided to define if weightage needs to be checked during rule evaluation (Auto-routing/Manual routing) If the Day 0 configuration is yes, then the rules will be evaluated irrespective of the currency. However, the final rule which is resolved will be as per the calculated weightage > If the Day 0 configuration is yes, then the rules will be evaluated irrespective of the currency. However, the final rule which is resolved will be as per the calculated weightage > If the Day 0 configuration is no, then he rules will be evaluated irrespective of the currency. All the rules falling within the amount range (post currency conversion) will be resolved. Whichever approver picks the transaction first, that rule will be the final resolved rule
Release Facility	Specify whether the release functionality is enabled or disabled at the Group Corporate level. The options are: • Enabled- it means the transaction release facility is enabled at Group Corporate level. If enabled, all the transactions as per the specified rule, will be sent for release to the configured users/user groups post successful approval at all levels • Disabled- it means the transaction release facility is disabled at Group Corporate level. If disabled, the transactions will not be sent to the releaser post successful approval at all levels
Corporate Administrator Facility	Set this flag if Corporate Admin facility is required for the Group Corporate.

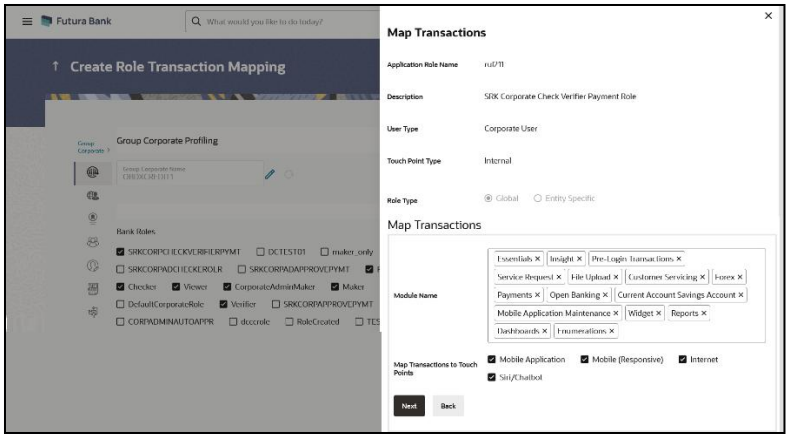
Field Name	Description
Accessible Roles for Corporate Administrator	Select the Roles that should be available to Corporate admin for onboarding new users

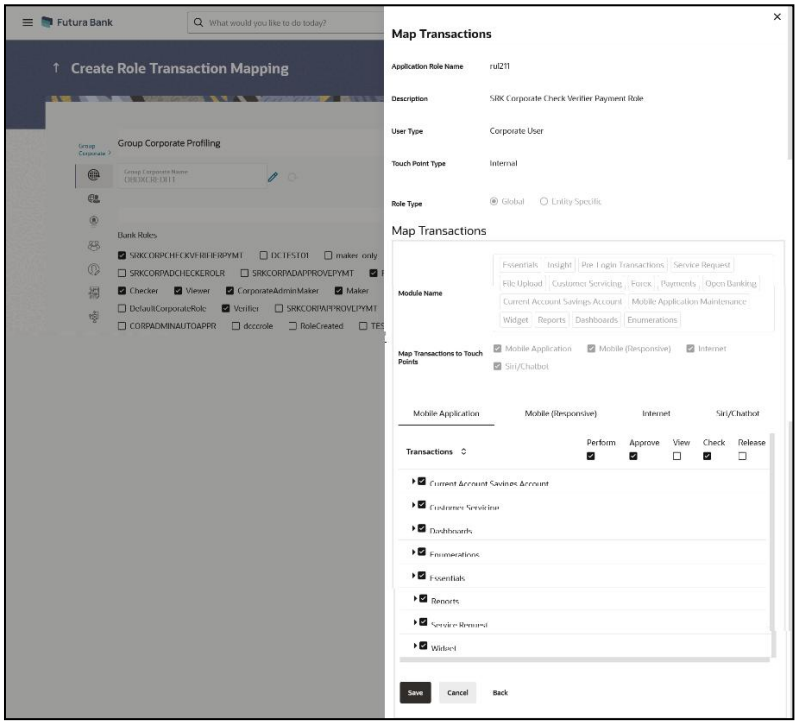
1. In the **Bank Role Name** field, select the checkbox (s) against the application roles and assign the **Application** Roles available at enterprise level (This Application roles are created using **Role Transaction Mapping** screen).
2. From the **Custom Role** list, select the roleif a custom role is required to be added for the Group Corporate.
3. Click **Add role** to create application role. The **Map Transaction** overlay screen appears.
4. The **Application Role Creation** screen to add transaction modules and touch points appears.
   OR
   Click **Cancel** to cancel the transaction and to go back to previous screen.

Create Custom Role - Application Role Creation

Using this option, System Administrator can select and assign the roles available at enterprise level as is, or can create a custom role for the Group Corporate by cloning a role available at Group Corporate level and map transactions to it for the selected touch points.

Application Role Creation





Field Description

Field Name	Description
Create Custom Role	
Application Role Name	Name of the application role.
Custom Application Role Name	Name for the Custom Application role.
Description	Displays the description of the application role.
User Type	Displays the user type for whom an application role is to be created.
Touch Point Type	Displays the touch point type for whom an application role is to be created.
Role Type	Displays the role type for whom an application role is to be created.
Map Transactions	
Module Name	The modules for which the transaction mapping is to be done. Transactions under the selected modules will get displayed for mapping
Map Transactions to Touch Points	The internal touch points for which the transaction mapping is done for application role. All the internal touch point maintained in the system gets displayed here. This field is displayed and enabled, only if you select the Internal option in the Touch Point Type field.
Transaction Name	Name of transaction to be mapped to the application role.

Field Name	Description
Action	Name of the action that can be performed for that transaction by the user to which this application role is assigned. • Perform- This action allows the user to perform or initiate that transaction and should be given to maker role. • Approve- This action allows the user to approve that transaction and should be provided to approval role • View- This action allows the user to view the initiated and approved transactions by other users and should be given to viewer role • Check- This action allows the user to check the initiated transactions by other users and should be given to checker role • Release- This action allows the user to release the initiated transactions by other users and should be given to releaser role

c. In the **Application Role Name** field, the existing application role from which the clone of the application role is being created will be displayed.

d. In the **Custom Application Role Name** field , enter the name of the application role.

e. Select appropriate **Module Name** for transactions mapping.

f. Select the check box against the list of **Touch Points** to map the transactions to selected touch points.

g. Click **Next** to proceed to next step.
OR
Click **Back** to go back to previous step.

h. To map the Transactions to the role, click ▸ against the particular module, then select the transaction type, and then transactions to be mapped

i. Select the respective check boxes preceding to transaction to be mapped.
OR
Select the checkbox at every transaction header level if you want to map all the transactions belong to that parent transactions at one instance.

j. Click **Save** to save the changes.
OR
Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate back to the previous screen.

1. Select the appropriate **Workflow Preference** to specify the preference to implement the workflow, whether at Corporate Level or at Rule Level.

k. If **Workflow Preference** is selected as **Corporate Level**;

v. Select the **Approval Flow** to define the Approval workflow type, if it has to be sequential or parallel or No Approval is required.

2. Select the **Approval Routing Type**;
   Select **Auto** if you wish system should resolve the rule and send the transaction for approval as per the rule resolved by the system.
   OR
   Select **Manual** if you wish to allow initiator to choose workflow from the resolved rules as part of transaction initiation.
3. Select the **Release Facility** flag if the release functionality needs to be enabled at Group Corporate level.
4. Select the **Corporate Administrator Facility** flag if Corporate Admin facility is required for the Group Corporate.
5. Select **Accessible Roles for Corporate Administrator** field, select the Roles that should be available to Corporate admin for onboarding new users.
6. Click **Save** to save the maintenance, and redirect to the review page.

   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.

Note: Admin can submit the maintenance after any step. Maintenances saved so far will be sent for approval in one flow. Admin would not be able to make any changes or maintain another step for the same Group Corporate till the time the approval of the wizard is not done.

7. The **Review** screen appears. Verify the details, and click **Submit**.
   OR
   Click **Edit** to modify the details entered.
   OR
   Click **Next** to proceed to next step.
   OR
   Click **Retain Draft** to save all the steps completed so far, and allow Admin resume the same application.
   OR
   Click **Cancel** to cancel the transaction.
8. The success message appears along with the transaction reference number.

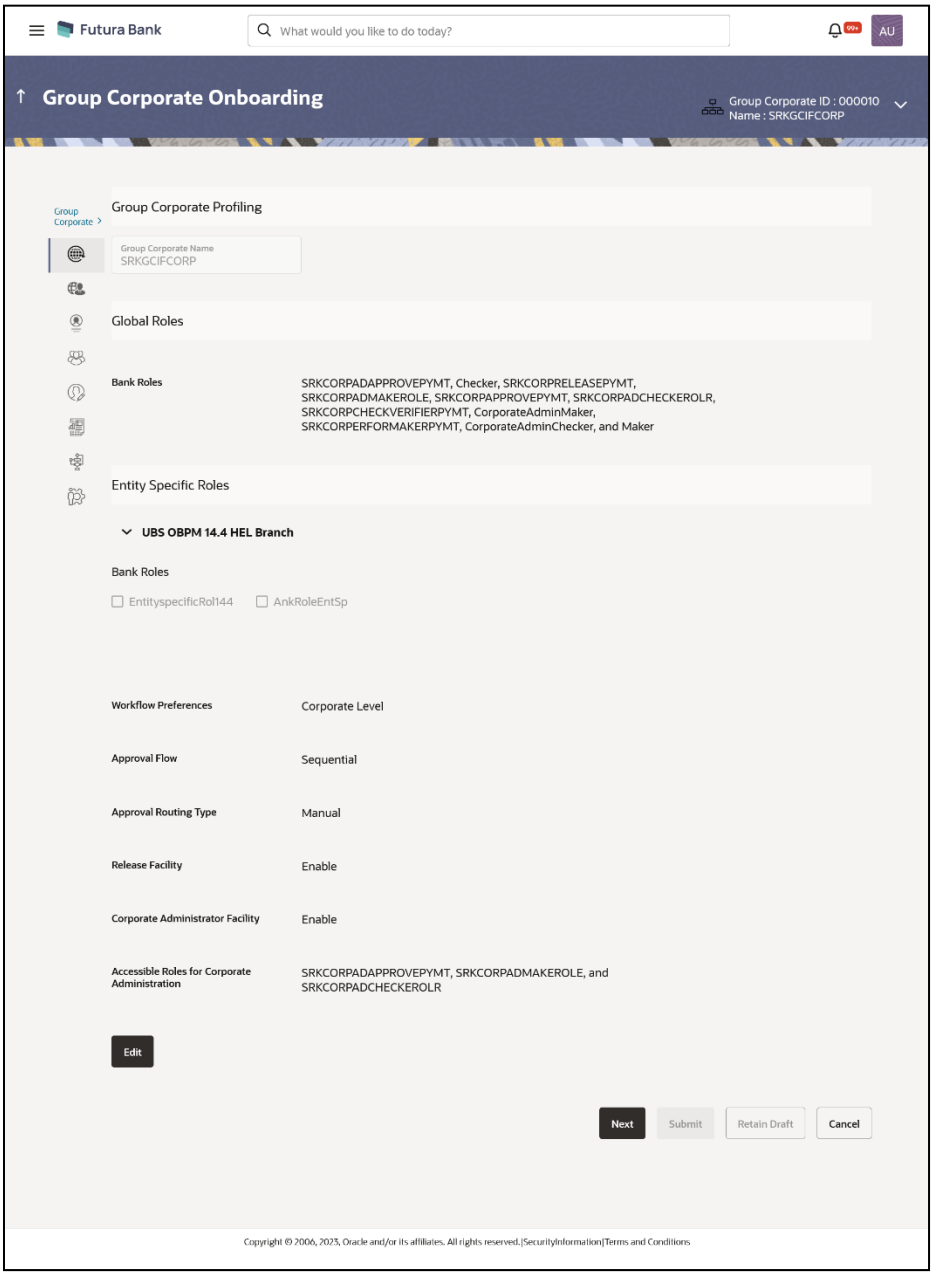
15.2.2 Group Corporate Profiling - View

Using this option, System/ Bank administrators can search and view profiling details of the existing Group Corporate.

To search and view Profiling details of the Group Corporate:

1. In the **Search By** field, select the appropriate option to search the Group Corporate.
   a. If you select the **Group Corporate** option;
      vi. In the **Group Corporate ID** field, enter the Group Corporate ID whose Group Corporate Details you wish to view.
      OR
      In the **Group Corporate Name** field, enter the name of the Group Corporate whose Group Corporate Details you want to view.
   b. If you select the **Party** option;
      i. In the **Party ID** field, enter the party ID mapped to Group Corporate you wish to view. The **Search Party** popup appears.
      ii. From the **Entity ID** list, select the entity from which party to be searched.
      iii. In the **Party ID** field, enter the party ID to be searched.
      OR
      In the **Party Name** field, enter the name of the party to be searched.
      iv. Click **Search** to search the party mapped to the Group Corporate.
      OR
      Click **Cancel** to cancel the transaction
      OR
      Click **Clear** to rest the entered details.
2. Click **Search**.
   The Group Corporate summary screen appears with search results as per the searched criteria.
   In case of invalid Group Corporate details, error message is shown on the screen.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
3. Click the link under the **Onboarding Status** or **Modification Status** column. The search result according to the search criteria appears

Group Corporate Profiling – View



Field Description:

Field Name	Description
Group Corporate Name	Name of the group corporate.

Field Name	Description
Global Role	
Bank Roles	Display all the roles mapped at Group Corporate level.
Entity Specific Roles	The roles associated with a particular entity. Note: • If an application role is assigned to an entity to which the administrator is not mapped, then the administrator is not able to access the role for view/modify/delete. • If a Group Corporate specific application role is created by extending an existing entity specific application role, the entity mapping applicable to the parent role from which the Group Corporate specific application role has been created, would be applicable to the Group Corporate specific application role. An administrator will not be able to modify the 'Entity' of custom application roles once created.
Custom Role	Display the custom role assigned for the Group Corporate (If any) by cloning a role available at Group Corporate level. **Note** : Admin will be able to assign a mix of bank roles and custom roles to a Group Corporate
Workflow Preferences	Display the workflow preference set up to implement the workflow. Possible values will be • Corporate Level • Rule Level
Approval Flow	Display the Approval workflow type, Possible values will be • Sequential • Parallel • No Approval This field is enabled if **Corporate Level** option is selected in **Workflow Preferences** field.

Field Name	Description
Approval Routing Type	Displays the approval routing type. Possible value will be • Auto • Manual Note: resolved rules as part of transaction initiation 1) In case system resolves multiple rules with different min-max slabs, then as per rule resolution logic, it will resolve the rule which has the nearest 'max' value in the defined slab. > A Day 0 configuration is provided to define if weightage needs to be checked during rule evaluation (Auto-routing/Manual routing) If the Day 0 configuration is yes, then the rules will be evaluated irrespective of the currency. However, the final rule which is resolved will be as per the calculated weightage >>If the Day 0 configuration is yes, then the rules will be evaluated irrespective of the currency. However, the final rule which is resolved will be as per the calculated weightage >>If the Day 0 configuration is no, then he rules will be evaluated irrespective of the currency. All the rules falling within the amount range (post currency conversion) will be resolved. Whichever approver picks the transaction first, that rule will be the final resolved rule
Release Facility	Displays the whether the release functionality is enabled or disabled at Group Corporate level.
Corporate Administrator Facility	Display the flag if Corporate Admin facility is maintained for the Group Corporate.
Accessible Roles for Corporate Administrator	Display the Roles that made available to Corporate admin for onboarding new users

View Custom Role - Application Role

Using this option, System Administrator can view the custom created application role details assigned for viewing Group corporate at enterprise level.

Field Description

Field Name	Description
View Customer Role	
Application Role Name	Name of the application role.
Custom Application Role Name	Name for the Custom Application role
Module Name	The modules for which the transaction mapping is done. Transactions under the selected modules will get displayed for mapping
Map Transactions to Touch Points	The internal touch points for which the transaction mapping is done for application role. All the internal touch point maintained in the system gets displayed here. This field is displayed and enabled, only if you select the Internal option in the Touch Point Type field.
Transaction Name	Name of transaction mapped to the application role.
Action	Name of the action that can be performed for that transaction by the user to which this application role is assigned. • Perform- This action allows the user to perform or initiate that transaction and should be provided to maker role. • Approve- This action allows the user to approve that transaction and should be given to approval role • View- This action allows the user to view the initiated and approved transactions by other users and should be given to viewer role • Check- This action allows the user to check the initiated transactions by other users and should be given to checker role • Release- This action allows the user to release the initiated transactions by other users and should be given to releaser role

4. Click **Back** to navigate back to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.

15.2.3 Group Corporate Profiling - Edit

This function enables administrator user to edit the exiting Group Corporate Profiling details.

To edit the Profiling details of the Group Corporate:

1. In the **Search By** field, select the appropriate option to search the Group Corporate.
   a. If you select the **Group Corporate** option;
      i. In the **Group Corporate ID** field, enter the Group Corporate ID whose Group Corporate Details you wish to view.
      OR
      In the **Group Corporate Name** field, enter the name of the Group Corporate whose Group Corporate Details you want to view.
   b. If you select the **Party** option;
      i. In the **Party ID** field, enter the party ID mapped to Group Corporate you wish to view. The **Search Party** popup appears.
      ii. From the **Entity ID** list, select the entity from which party to be searched.
      iii. In the **Party ID** field, enter the party ID to be searched.
      OR
      In the **Party Name** field, enter the name of the party to be searched.
      iv. Click **Search** to search the party mapped to the Group Corporate.
      OR
      Click **Cancel** to cancel the transaction
      OR
      Click **Clear** to rest the entered details.

1. Click **Search**.
   The Group Corporate summary screen appears with search results as per the searched criteria.
   In case of invalid Group Corporate details, error message is shown on the screen.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
2. Click the link under the Onboarding Status or Modification Status column. The search result according to the search criteria appears.

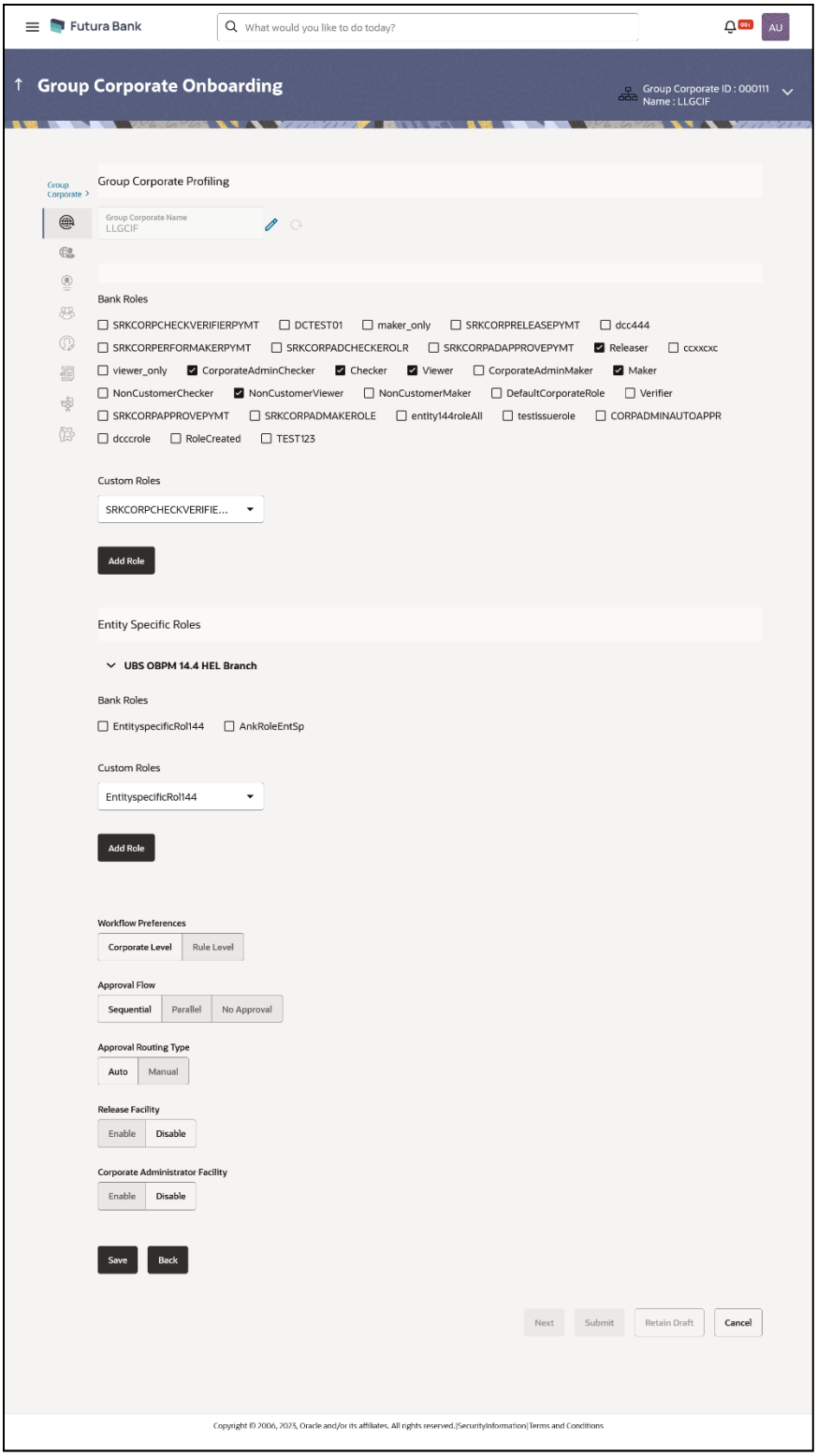
3. Click on the icon adjacent to **Group Corporate Name** field to modify the name of the Group Corporate.

    a. Enter the new Group Corporate name, and click **Check Availability** to check the uniqueness of the name.

Note: If the user ID is already used.
1) Displays **Available** status if new name assigned is unique and can be used.

2) The icon is provided to reset and re-enter the new name.
3) If user clicks on save without checking the availability, system displays the an error message.

Group Corporate Profiling – Edit



Field Description

Field Name	Description
Group Corporate Name	Name of the group corporate. This field is editable.
Global Role	
Bank Roles	All the roles available at enterprise level. This field is editable.
Customer Roles	Create a custom role for the Group Corporate by cloning a role available at Group Corporate level. This field is editable. **Note** : Admin will be able to assign a mix of bank roles and custom roles to a Group Corporate.
Entity Specific Roles	The roles associated with a particular entity. This field is editable. Note: • If an application role is assigned to an entity to which the administrator is not mapped, then the administrator is not able to access the role for view/modify/delete. • If a Group Corporate specific application role is created by extending an existing entity specific application role, the entity mapping applicable to the parent role from which the Group Corporate specific application role has been created, would be applicable to the Group Corporate specific application role. An administrator will not be able to modify the 'Entity' of custom application roles once created.
Customer Roles	Create a custom role for the Group Corporate by cloning a role available at Group Corporate level. This field is editable. **Note** : Admin will be able to assign a mix of bank roles and custom roles to a Group Corporate

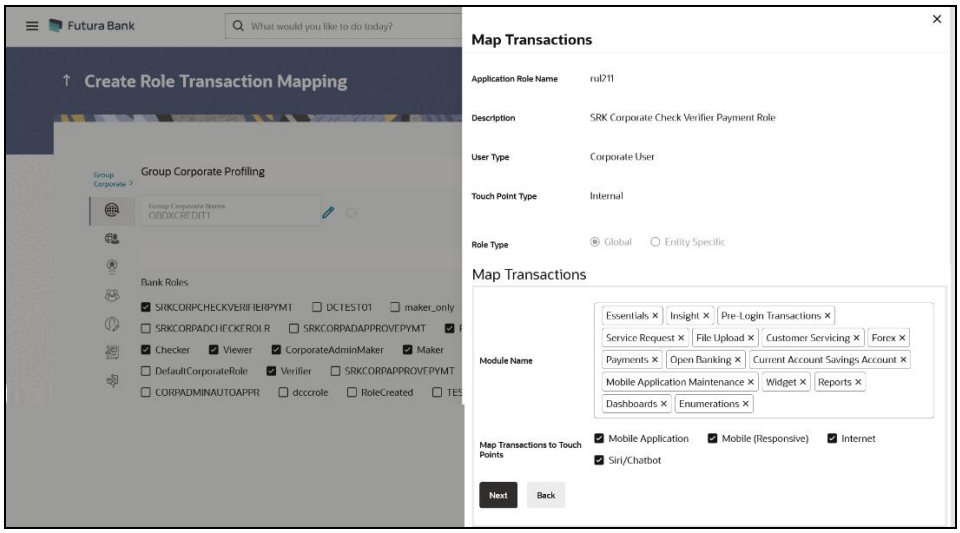
Field Name	Description
Workflow Preferences	The preference to implement the workflow. This field is editable. Possible value will be: • Corporate Level • Rule Level
Approval Flow	Define the Approval workflow type. This field is editable. Possible value will be: • Sequential • Parallel • No Approval This field enable if **Corporate Level** option is selected in **Workflow Preferences** field.

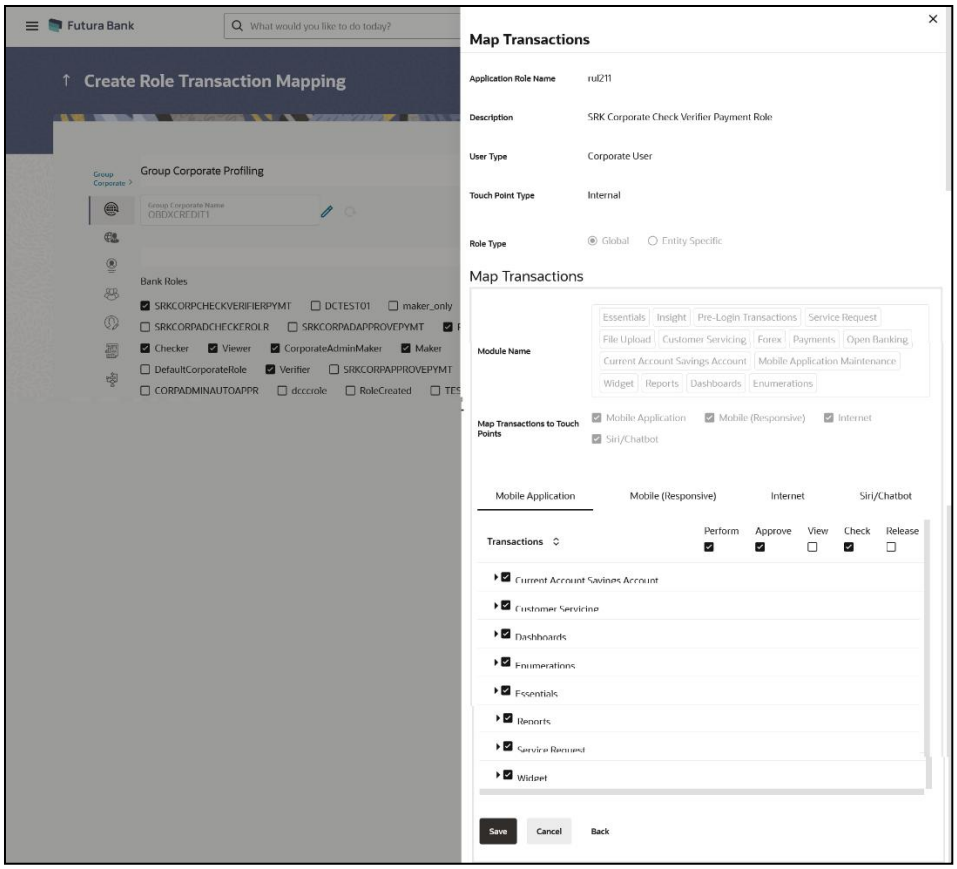
Field Name	Description
Approval Routing Type	Define the approval routing type. This field is editable. Possible value will be: • Auto- System will resolve the rule and the transaction will be sent for approval as per the rule resolved by the system. A rule which is having amount slab closest to the transaction amount will be resolved. The user will not have an option to select the approval workflow if routing type is Auto • Manual- User will be able to select a workflow from the resolved rules as part of transaction initiation Note: 1) In case system resolves multiple rules with different min-max slabs, then as per rule resolution logic, it will resolve the rule which has the nearest 'max' value in the defined slab. > A Day 0 configuration is provided to define if weightage needs to be checked during rule evaluation (Auto-routing/Manual routing) If the Day 0 configuration is yes, then the rules will be evaluated irrespective of the currency. However, the final rule which is resolved will be as per the calculated weightage >>If the Day 0 configuration is yes, then the rules will be evaluated irrespective of the currency. However, the final rule which is resolved will be as per the calculated weightage >>If the Day 0 configuration is no, then he rules will be evaluated irrespective of the currency. All the rules falling within the amount range (post currency conversion) will be resolved. Whichever approver picks the transaction first, that rule will be the final resolved rule
Release Facility	Specify whether the release functionality is to be enabled or disabled at Group Corporate level. This field is editable.
Corporate Administrator Facility	Set this flag if Corporate Admin facility is required for the Group Corporate. This field is editable.
Accessible Roles for Corporate Administrator	Select the Roles that should be available to Corporate admin for onboarding new users. This field is editable.

4. In the **Bank Role Name** field, select the checkbox (s) against the application roles and assign the Application **Roles** available at enterprise level (This Application roles are created using Role Transaction Mapping screen).
5. From the **Custom Role** list, select the role, if a custom role is required to be added for the Group Corporate.
6. Click **Add role** to create application role. The **Map Transaction** overlay screen appears.
7. The **Application Role Creation** screen to add transaction modules and touch points appears.
   OR
   Click **Cancel** to cancel the transaction and to go back to previous screen.

Create Customer Role - Application Role Creation

Using this option, System Administrator can select and assign the roles available at enterprise level as is, or he can create a custom role for the Group Corporate by cloning a role available at Group Corporate level and map transactions to it for selected touch points.





Field Description

Field Name	Description
Create Customer Role	
Application Role Name	Name of the application role.
Custom Application Role Name	Name for the Custom Application role
Module Name	The modules for which the transaction mapping is to be done. Transactions under the selected modules will get displayed for mapping

Field Name	Description
Map Transactions to Touch Points	The internal touch points for which the transaction mapping is done for application role. All the internal touch point maintained in the system gets displayed here. This field is displayed and enabled, only if you select the Internal option in the Touch Point Type field.
Transaction Name	Name of transaction to be mapped to the application role.
Action	Name of the action that can be performed for that transaction by the user to which this application role is assigned. • Perform- This action lets the user to perform or initiate that transaction and should be given to maker role. • Approve- This action lets the user to approve that transaction and should be given to approval role • View- This action lets the user to view the initiated and approved transactions by other users and should be given to viewer role • Check- This action allows the user to check the initiated transactions by other users and should be given to checker role • Release- This action allows the user to release the initiated transactions by other users and should be given to releaser role

a. In the **Application Role Name** field, the existing application role from which the clone of the application role is being created will be displayed.

b. In the **Custom Application Role Name,** enter the name of the application role.

Note: Enter the new **Custom Application Role Name**, and click **Check Availability** to check the uniqueness of the name.

c. Select appropriate **Module Name** for transactions mapping.

d. Select the check box against the list of Touch Points to map the transactions to selected touch points.

e. Click **Next** to proceed to next step.
OR
Click **Back** to go back to previous step.

f. To map the **Transactions** to the role, click against the particular module, then select the transaction type, and then transactions to be mapped

g. Select the respective check boxes preceding to transaction to be mapped.
OR
Select the checkbox at every transaction header level if you want to map all the transactions belong to that parent transactions at one instance.

h. Click **Save** to save the changes.
OR
Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate back to the previous screen.

8. Select the appropriate **Workflow Preference** to specify the preference to implement the workflow, whether at Corporate Level or at Rule Level.

   i. Select the **Approval Flow** to define the Approval workflow type, if it has to be sequential or parallel or No Approval is required.

9. Select the **Approval Routing Type**;
Select **Auto** if you wish system should resolve the rule and send the transaction for approval as per the rule resolved by the system.
OR
Select **Manual** if you wish to allow initiator to choose workflow from the resolved rules as part of transaction initiation.

10. Select the **Release Facility** flag if the release functionality needs to be enabled at Group Corporate level

11. From the **Accessible Roles for Corporate Administrator** field, select the roles that should be available **to Corporate Administrator** for onboarding new users.

1. Click **Save** to save the maintenance, and redirect to the review page.
OR
Click **Next** to proceed to the next logical step.
OR
Click **Submit** to submit the steps performed so far for approval.
OR
Click **Retain Draft** to save the details entered as draft.
OR
Click **Cancel** to cancel the transaction.

Note: Admin can submit the maintenance after any step. Maintenances saved so far will be sent for approval in one flow. Admin would not be able to make any changes or maintain another step for the same Group Corporate till the time the approval of the wizard is not done.

---

2. The **Review** screen appears. Verify the details, and click **Submit**.
OR
Click **Edit** to modify the details entered.
OR
Click **Next** to proceed to next step.
OR
Click **Retain Draft** to save all the steps completed so far, and allow Admin resume the same application.
OR
Click **Cancel** to cancel the transaction.

3. The success message appears along with the transaction reference number.

15.3 Step 2: Party Account Access

System/Bank Administrator can set up account and transaction access at the Group corporate level. The System/ Bank Administrator can provide access to accounts held by the corporate parties associated with Group corporate with as available in the core banking application or the respective mid-office application.

Bank administrator can set up the Account access for multiple corporate parties under Group Corporate a single step

Using this function system administrator can manage access for Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts along with Liquidity Management enabled Real Accounts (including External Accounts if any) and VAM enabled Real and virtual accounts for a Corporate.

Upon navigating to the specific category tab viz. Demand Deposits, Term Deposits, Loans etc., the administrator can select a global check box of 'Map accounts' for All ,to enable all the existing accounts under the selected category for channel banking. If specific accounts are required to be given access then the user needs to select the respective check boxes preceding the account number.

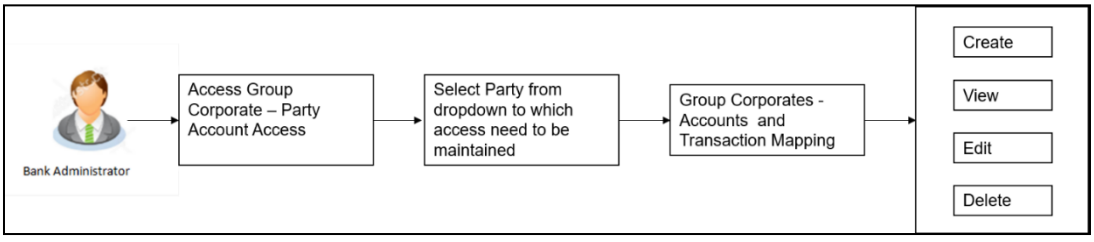
Note: Access Management for Loan Accounts is for accounts fetched from Core Banking System i.e. FCUBS. It is not supported for accounts from Oracle Banking Corporate Loan (OBCL) system.

As part of this maintenance, Accounts and Transaction mapping maintenance can be done for all the corporate party ID mapped under Group Corporate in a single step.

Pre-Requisites

- Party preferences should be created for the party for which access is to be maintained
- Channel Access should be enabled for party for which account access is to be maintained
- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.

Workflow



Features Supported In Application

The following options are available as part of this maintenance:

- Party Account Access - Mapping
- Party Account Access – View
- Party Account Access - Edit
- Party Account Access - Delete

How to reach here:

System/ Bank Administrator Dashboard > Corporate Onboarding > Group Corporate Onboarding > Party Account Access

OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Group Corporate Onboarding > Party Account Access

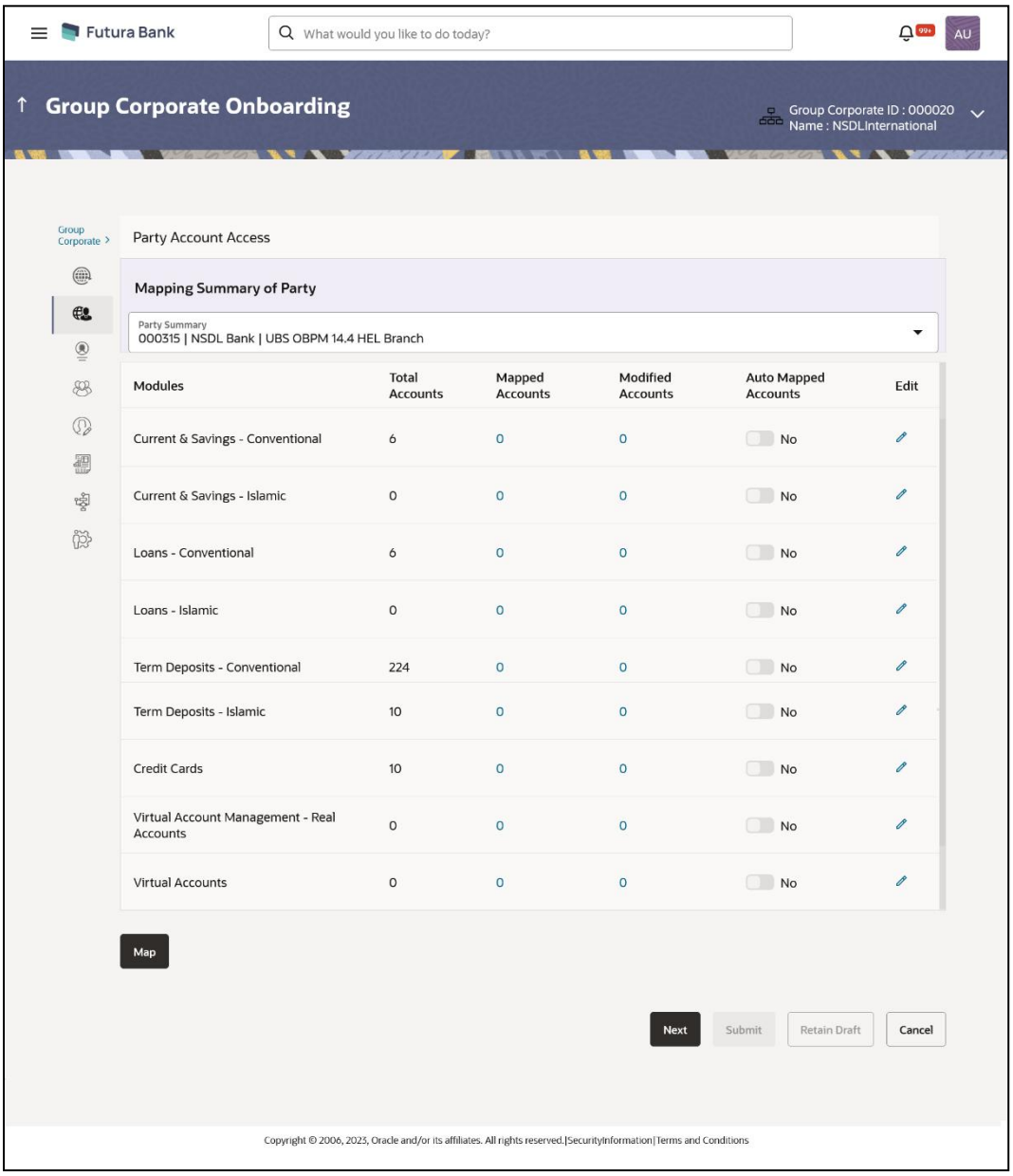
15.3.1 Party Account Access – Create

Using this option, Bank Administrator can maintain Accounts and Transaction access for the corporate parties associated with a specific Group Corporate ID.

To provide the corporate party (Associated to Group Corporate) with account and transaction access:

1. From the **Mapping Summary of Party** dropdown list, select the corporate party id.
2. For a searched party, summary screen will be displayed with total accounts associated with corporate party, status of the accounts mapped for the internet banking, modified accounts if any and Auto account mapping status.

Mapping Summary of Party .



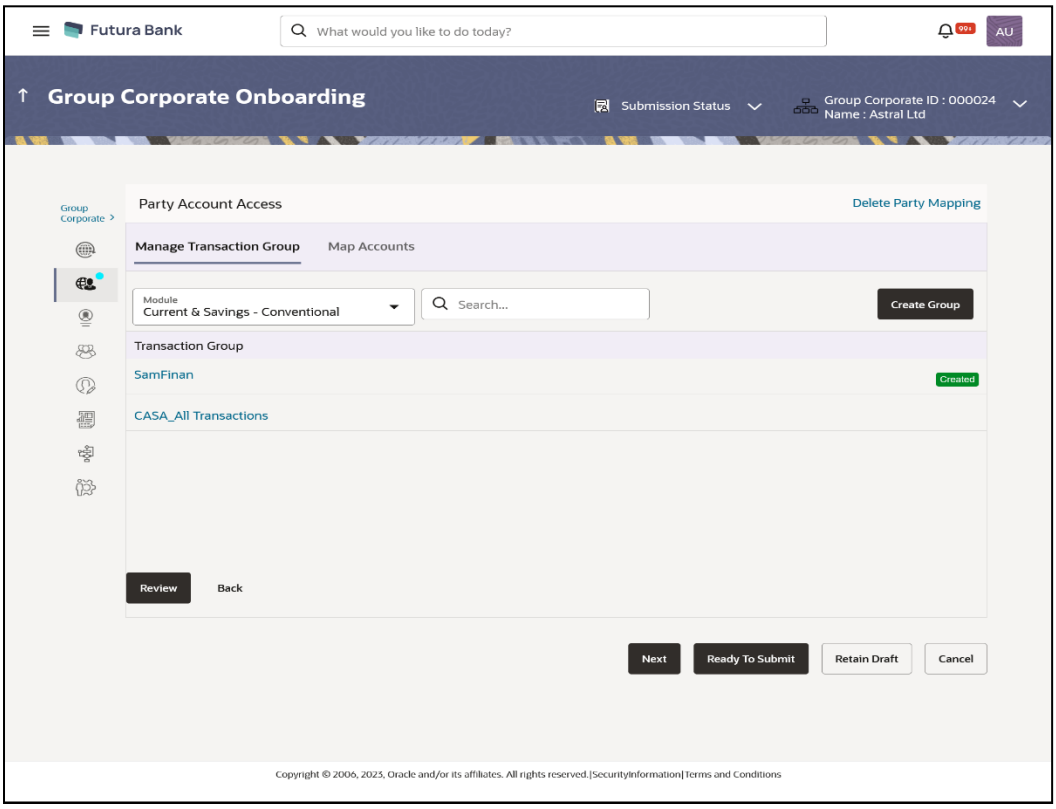
Field Description

Field Name	Description
Mapping Summary of Party	The corporate party for which Party accounts access is being viewed
Modules	Banking Module names

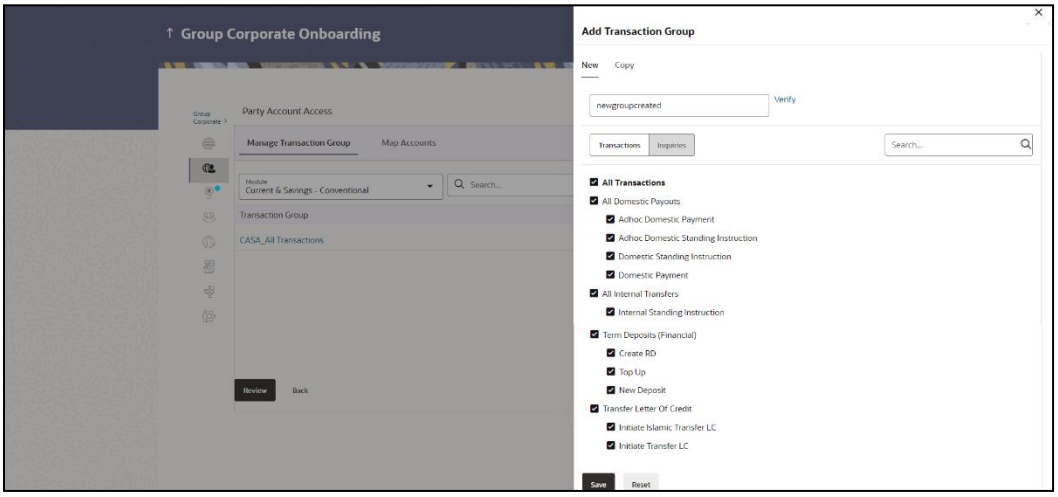
Field Name	Description
Total Accounts	Total number of accounts available under the party.
Mapped Accounts	Number of accounts mapped to the particular account type.
Modified Accounts	Number of accounts modified for the particular account type.
Auto Mapped Accounts	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided
Edit or Map	Click on the icon next to every module or click on Map button to edit party account access

3. If there is no mapping done for a party, the count for the **Mapped Accounts** will be '**0'**
4. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories i.e. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts along with Liquidity Management enabled Real Accounts (including External Accounts if any) and VAM enabled Real and virtual accounts for a Corporate.
5. Click **Map** or **Edit** (available across each banking module). The **Party Account Access - Create** screen appears.
   OR
   Click **Cancel** to cancel the transaction.

Party Account Access (Create) – Manage Transaction Group tab



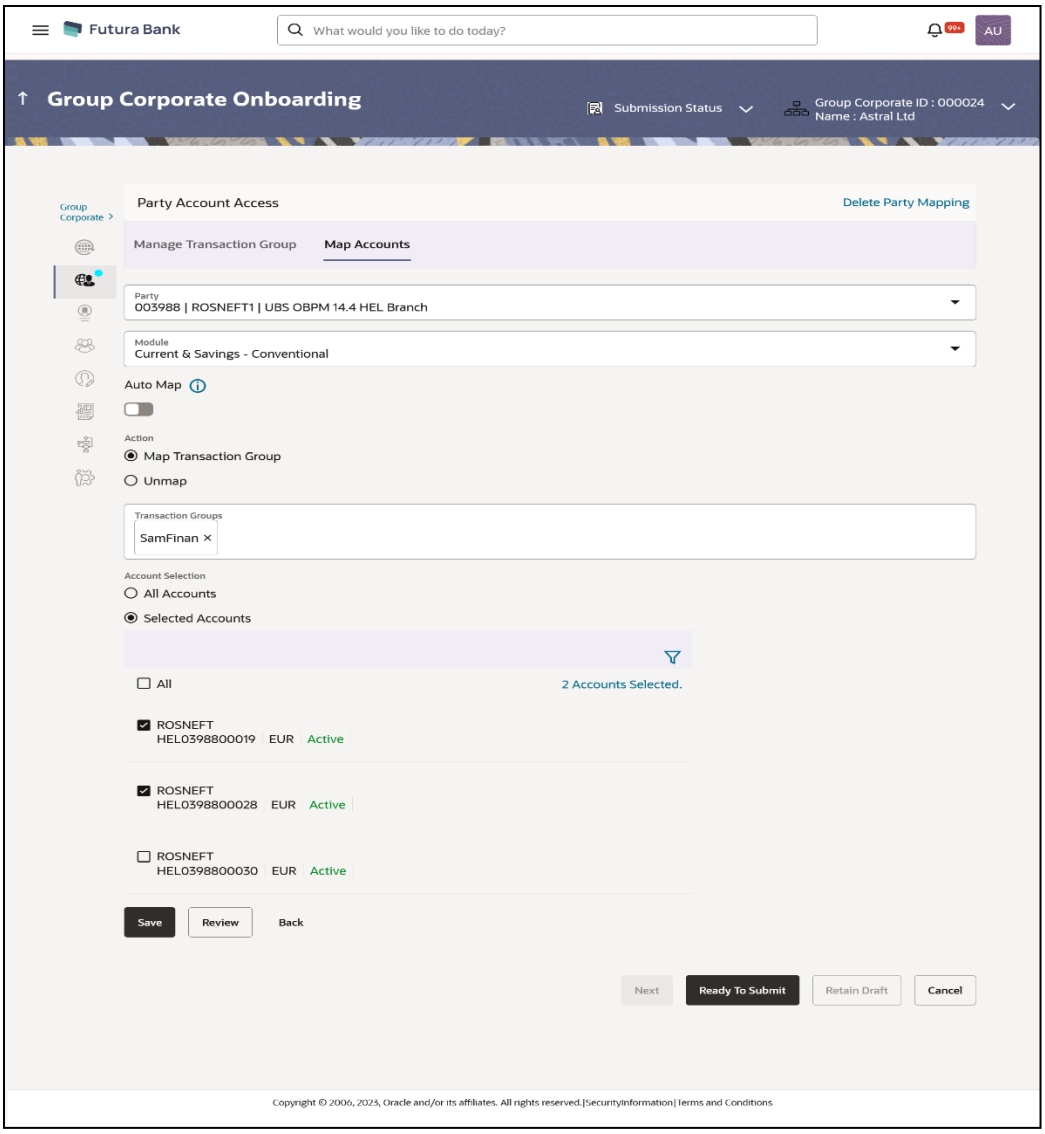
Add Transaction Group



Field Description:

Field Name	Description
Manage Transaction Group tab	
Modules	Select Banking Module to setup account access.
Select Transaction Groups	Select the Transaction group to map transactions and maintaining access in Account Access screens.
Add Transaction Group	Create a new transaction group by clicking the 'ADD' button. Note : • A new group can also be created by cloning/copying an existing transaction group • Multiple transaction groups can be created. • Transaction groups of one Group Corporate will be available for selection only for that Group Corporate
Following fields appears in overlay window when user click on **Add** to add new transaction group	
Name of Transaction Group	Specify the new transaction group to map transactions. Click **Verify** to check the availability the specific Transaction Group name.

Party Account Access (Create) – Map Accounts tab


Futura Bank
What would you like to do today?
AU
Group Corporate Onboarding
Submission Status
Group Corporate ID : 000024
Name : Astral Ltd
Party Account Access
Delete Party Mapping
Manage Transaction Group
Map Accounts
Party
003988 | ROSNEFT1 | UBS OBPM 14.4 HEL Branch
Module
Current & Savings - Conventional
Auto Map
Action
Map Transaction Group
Unmap
Transaction Groups
SamFinan
Account Selection
All Accounts
Selected Accounts
All
2 Accounts Selected.
ROSNEFT
HEL0398800019 EUR Active
ROSNEFT
HEL0398800028 EUR Active
ROSNEFT
HEL0398800030 EUR Active
Save
Review
Back
Next
Ready To Submit
Retain Draft
Cancel
Copyright © 2006, 2023, Oracle and/or its affiliates. All rights reserved.|SecurityInformation| Terms and Conditions

Field Description:

Field Name	Description
Map Accounts tab	
Party	Select the party to map accounts.
Module	Select Banking Module to setup account access.
Auto Map	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided
Action	Select the action to be done for selected transaction group. The options are: • Map Transaction Group: Select Transaction Group, then select the account numbers and then click on Save to map the transaction groups to the selected accounts. Multiple transactions can be mapped • Unmap: Select Unmap option, specify the transaction group to be unmapped and then select the accounts. On clicking Save, the selected transaction group will be unmapped from the account/accounts.. Note: Only one transaction group can be unmapped at a time. A transaction group can be unmapped from All Accounts or Selected Accounts.
Transaction Group	Select one or multiple transaction group/s to be mapped to the selected accounts. Select one transaction group to be unmapped from the selected account/accounts.

Field Name	Description
Account Selection	Select the account numbers to be mapped to the Transaction groups. User can select all the accounts available under selected party ID or click on filter and select the specific accounts. Note : 1) System will show a tag as 'Modified' followed by the transaction group name after the account number. 2) System displays the Account Number along with the Account Name, Account Currency, and Branch Code.
Delete Party Mapping	Click on **Delete Party Mapping** to delete all the Transaction and party account access maintenance done for corporate party all at once

6. The Party Account Access screen has two tabs. Header of the screen shows the Group Corporate Name and Group ID. The manage Transaction Group tab lists down all the **modules, transaction groups** created.
7. Navigate and select specific **module** tab (Including viz. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts along with Liquidity Management enabled Real Accounts (including External Accounts if any) and VAM enabled Real and virtual accounts for a Corporate.) in the first column for which account and transaction access mapping maintenance need to be setup.
8. The user can create a new **transaction group** by clicking the **'ADD'** button. On clicking **Add**, a new overlay will open where all the transactions and inquiries will be listed. User can provide a name the group and select the required transactions and inquiries and click the **save** button.
   OR
   Click **Reset** to clear added details in overlay screen.
9. A new group can also be created by **cloning/copying an existing transaction group**. Once the user selects an existing **transaction group**, system will populate the screen with the transactions selected in the copied group in editable mode. User can select or deselect some of the transactions as per his requirements and create a new group by providing a different transaction group name
10. There will be one factory shipped **Transaction group** for each module, which will have all transactions and inquiries grouped together.

Note: Factory shipped user group cannot be deleted or modified.

11. Once the transaction group/s are created, user can map these transaction groups to one or multiple accounts . Click on **Map Accounts** tab and select Party, then select Transaction Groups, select the account numbers and then click on **Save** to map the transaction groups to the selected accounts.
12. Click on the **Transaction Group link**, to view the list of transactions within the mapped transaction group in an overlay.
13. Select ‘All Accounts’ option to map/ unmap transaction groups from all accounts.
    OR

If specific accounts are required to be mapped, then select the respective check boxes preceding the account number.

14. Once the user maps the accounts, system will show a tag as **'Modified'** followed by the transaction group name after the account number.
15. To map the new accounts, select appropriate option from **Auto Map toggle button**;
    Select **Auto** if you wish to allow access to all future Accounts across banking module.
    OR
    Select **Manual** if you wish to explicitly map new accounts and transactions.
16. User can **unmap** the transaction groups by selecting accounts and then clicking on **Save** button to reset their mapping .
17. User can click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate party in one step.
18. User can drill down his search by applying Filter to search an account basis on the account number, transaction group, account access status, account status and currency
19. Click **Save** to save the maintenance, and redirect to the review page.
    OR
    Click **Next** to proceed to the next logical step.
    OR
    Click **Submit** to submit the steps performed so far for approval.
    OR
    Click **Retain Draft** to save the details entered as draft.
    OR
    Click **Cancel** to cancel the transaction.

Note: Admin can submit the maintenance after any step. Maintenances saved so far will be sent for approval in one flow. Admin would not be able to make any changes or maintain another step for the same Group Corporate till the time the approval of the wizard is not done.

20. The **Review** screen appears. Verify the details, and click **Submit**.
    OR
    Click **Edit** to modify the details entered.
    OR
    Click **Next** to proceed to next step.
    OR
    Click **Retain Draft** to save all the steps completed so far, and allow Admin resume the same application.
    OR
    Click **Cancel** to cancel the transaction.
21. The success message of user creation appears along with the transaction reference number

15.3.2 Party Account Access- View

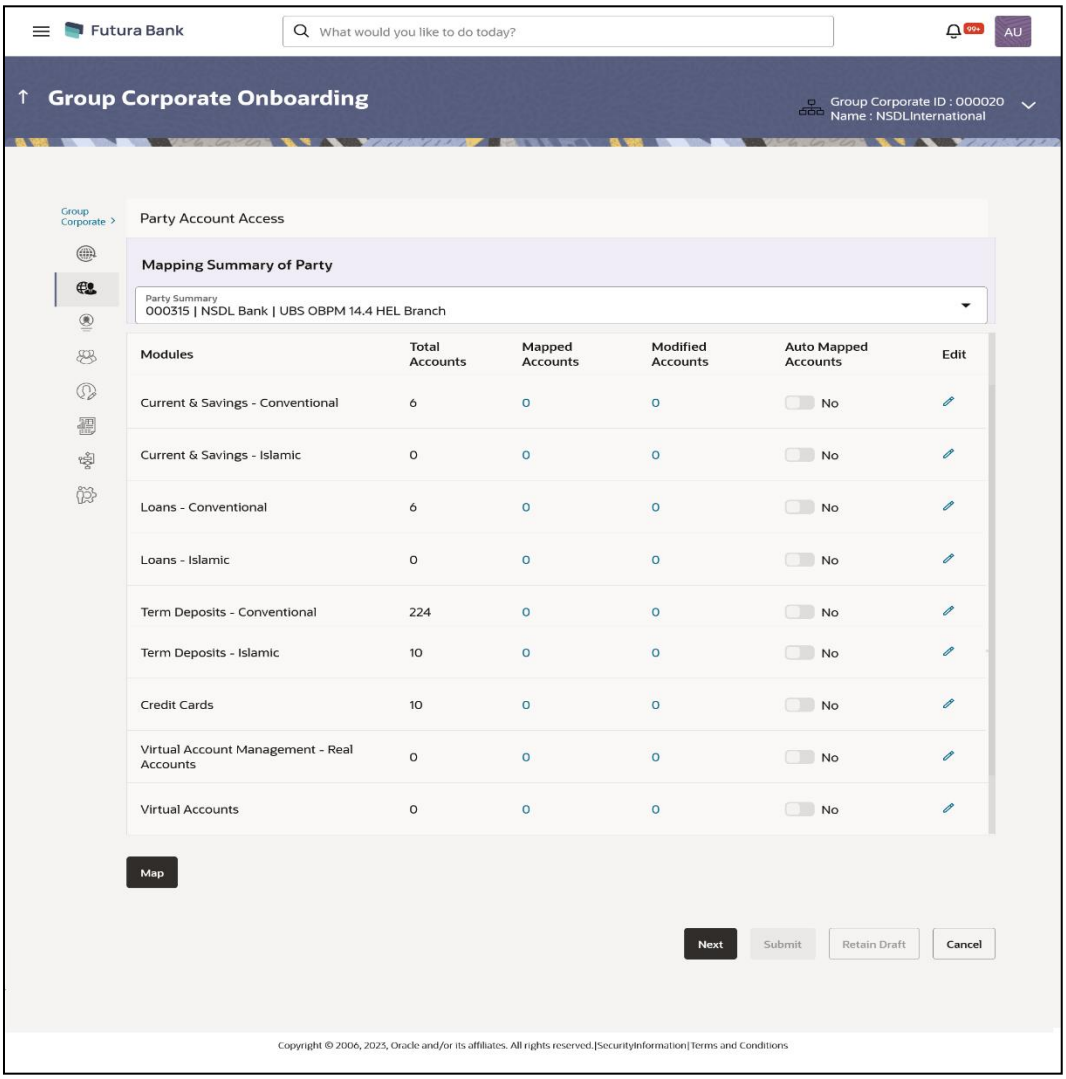
The Bank Administrator can view the list of account(s) and transactions for which access has been provided to the party.

To Search and view the party account and transaction access:

1. From the **Mapping Summary of Party** dropdown list, select the corporate party id.

2. For a searched party, summary screen will be displayed with total accounts associated with corporate party, status of the accounts mapped for the internet banking, modified accounts if any and Auto account mapping status .
3. Click the link under the total **Mapped accounts** or **Modified accounts**, The **Party Account Access – View** (Transaction Mapping) screen appears. The search result according to the search criteria appears
   OR
   Click **Cancel** to cancel the transaction.

Party Account Access - Summary Results



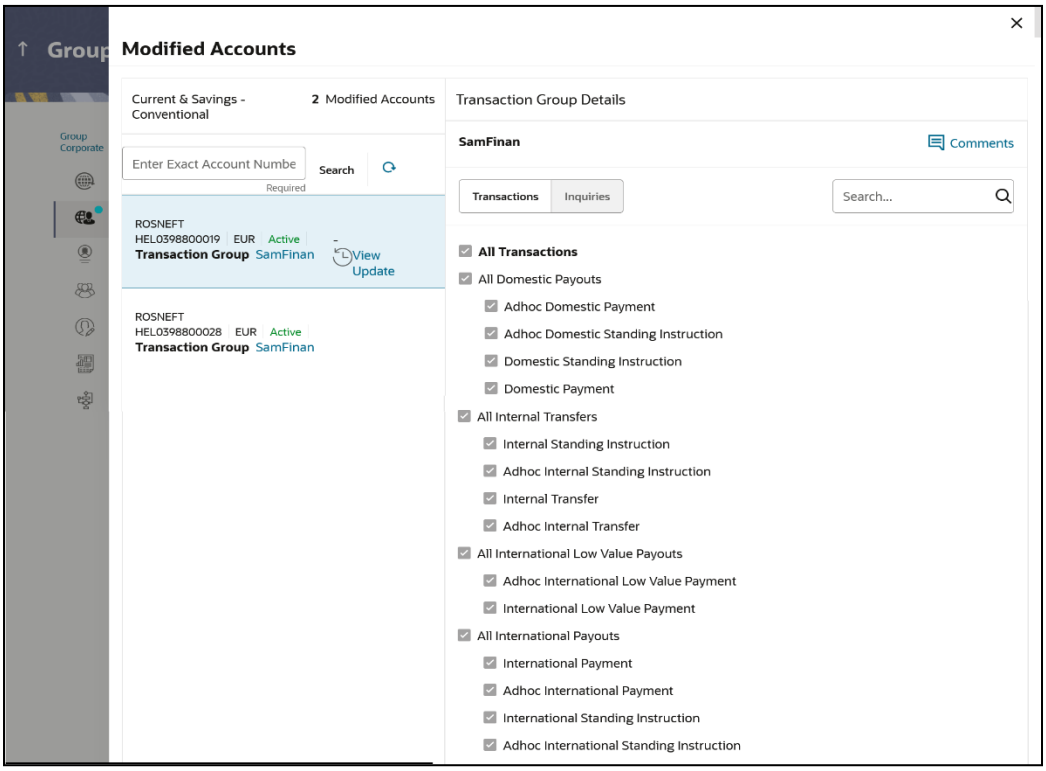
Field Description

Field Name	Description
Mapping Summary of Party	The corporate party for which Party accounts access is being viewed
Modules	Banking Module names
Total Accounts	Total number of accounts available under the party.
Mapped Accounts	Number of accounts mapped to the particular account type.

Field Name	Description
Modified Accounts	Number of accounts modified for the particular account type.
Auto Mapped Accounts	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided
Edit or Map	Click on the icon next to every module or click on Map button to edit party account access

4. If there is no mapping done for a party, the count for the **Mapped Accounts** will be '**0**'
5. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories

Party Account Access – View



Field Description:

Field Name	Description
Modules	Display name of the product for which account access is being viewed.
Mapped Accounts	Display Account number associated with corporate party, and the mapped transaction groups • Display account number along with the name, currency and status of the account as Active or Inactive. The mapped transaction group names can also be viewed against each account
Transaction Groups Details	Display the Transaction group details which are mapped to each account of the selected party. The details of the transaction group includes information related to transactions and inquiries.

6. The Party Account Access details screen has two sections. First column lists down all the Account numbers mapped with the corporate party, including Status of the account (Active or Inactive) and transaction group name
7. In the second column, user can view the **transaction group** details with all the transactions and inquiries access.
8. Click **Cancel** to cancel the transaction.
9. Click **Edit / Map** to update the **Party Account Access** account mapping for new accounts and existing accounts.
   OR
   Click **Cancel** to cancel the transaction.
10. Click **Next** to proceed to the next logical step.
    OR
    Click **Submit** to submit the steps performed so far for approval.
    OR
    Click **Retain Draft** to save the details entered as draft.
    OR
    Click **Cancel** to cancel the transaction.

15.3.3 Party Account Access- Edit

The Bank Administrator gets a request with the list of account(s) and transactions for which access details needs to be edited for the party.

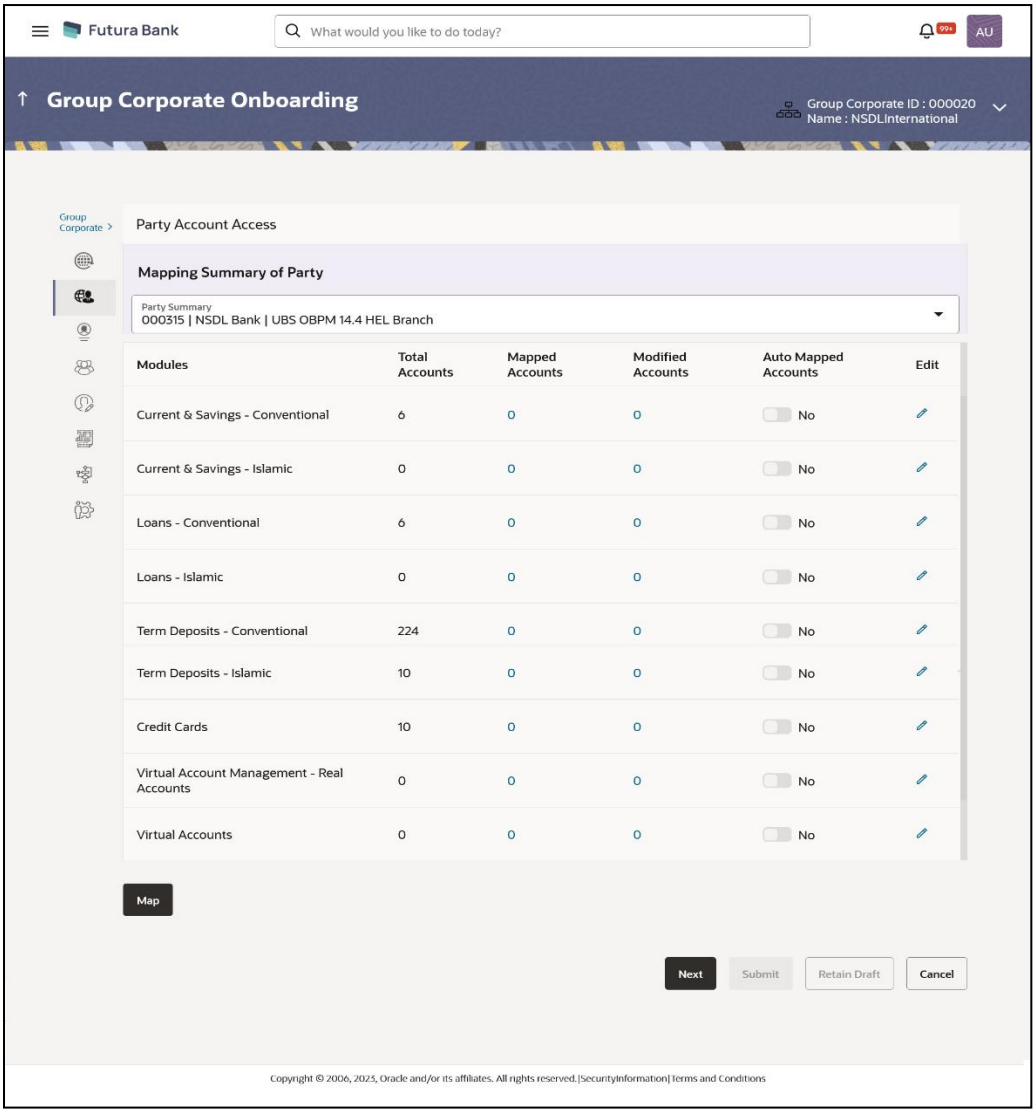
To Search and Edit the party account and transaction access:

1. From the **Mapping Summary of Party** dropdown list, select the corporate party id.
2. For a searched party, summary screen will be displayed with total accounts associated with corporate party, status of the accounts mapped for the internet banking, modified accounts if any and Auto account mapping status .
3. Click the link under the total **Mapped accounts** or **Modified accounts**, The **Party Account Access – View** (Transaction Mapping) screen appears. . The search result according to the

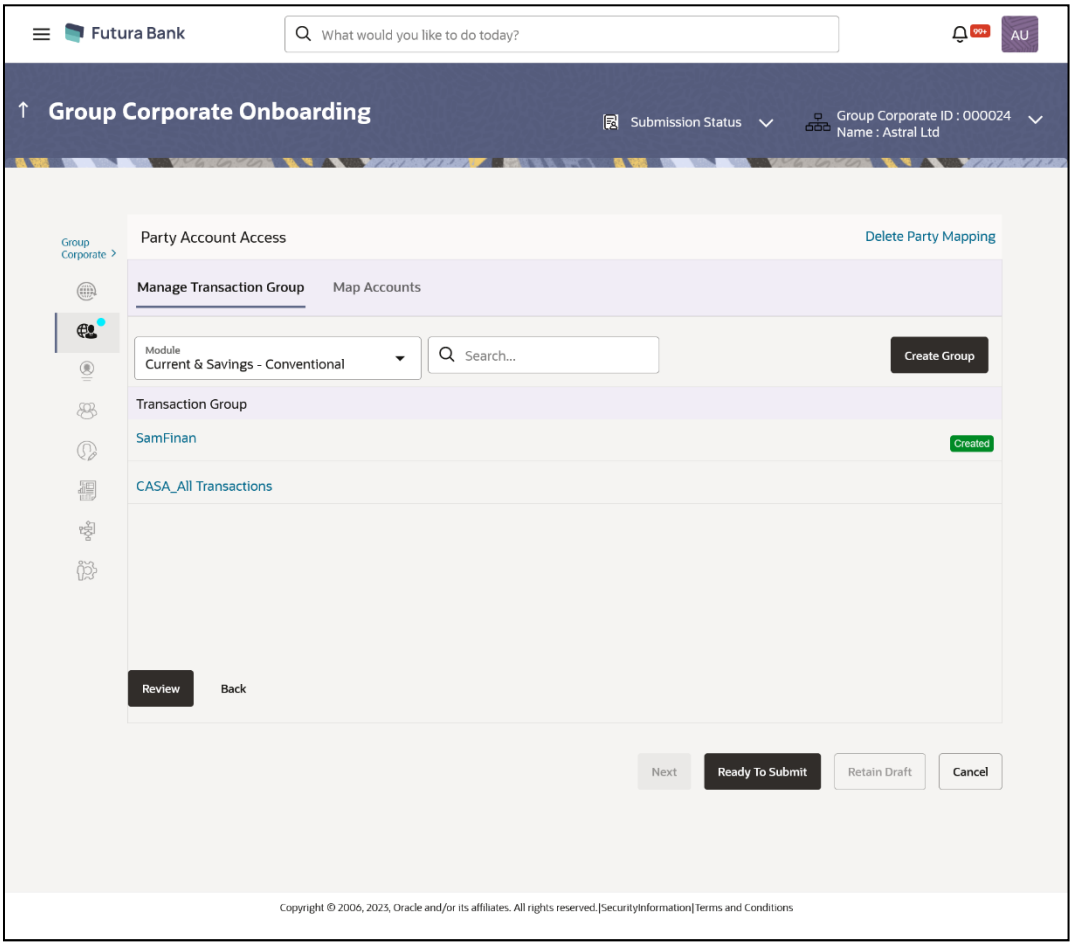
search criteria appears
OR
Click **Cancel** to cancel the transaction.

4. If there is no mapping done for a party, the count for the **Mapped Accounts** will be '**0'**
5. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories
6. Click **Map** or **Edit** (available across each banking module). The **Party Account Access - Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.

Party Account Access – Edit



Party Account Access – Edit Details



7. The Party Account Access screen has two tabs. Header of the screen shows the Group Corporate Name and Group ID. The manage Transaction Group tab lists down all the **modules, transaction groups** created.

8. Navigate and select specific **module** tab (Including viz. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts along with Liquidity Management enabled Real Accounts (including External Accounts if any) and VAM enabled Real and virtual accounts for a Corporate.) in the first column for which account and transaction access mapping maintenance need to be setup.

9. The user can create a new **transaction group** by clicking the **'ADD'** button. On clicking **Add**, a new overlay will open where all the transactions and inquiries will be listed. User can provide a name the group and select the required transactions and inquiries and click the **save** button.
   OR
   Click **Reset** to clear added details in overlay screen.

10. A new group can also be created by **cloning/copying an existing transaction group**. Once the user selects an existing **transaction group**, system will populate the screen with the transactions selected in the copied group in editable mode. User can select or deselect some

of the transactions as per requirements and create a new group by providing a different transaction group name

11. There will be one factory shipped **Transaction group** for each module, which will have all transactions and inquiries grouped together.

Note: Factory shipped user groups cannot be deleted or modified.

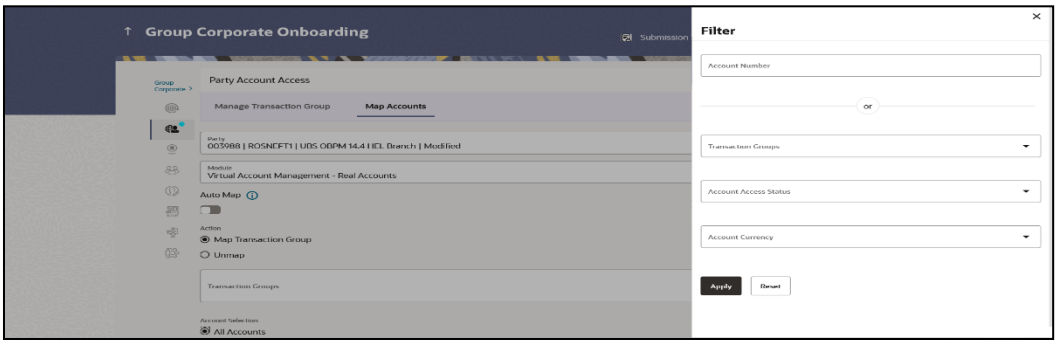
12. Once the transaction groups are created, user can select specific module , along with the transaction groups and can select 'All Accounts' to map the selected transaction group/s to all the existing accounts under the selected party
    OR
    If transaction groups need to be mapped to specific accounts, then the user needs to select the respective check boxes preceding the account number.
13. Once the user maps the accounts, system will show a tag as **'Modified'** followed by the transaction group name after the account number.
14. To map the new accounts, select appropriate option from **Auto Map** toggle button;
    Select **Auto** if you wish to allow access to all future Accounts across banking module.
    OR
    Select **Manual** if you wish to explicitly map new accounts and transactions.
15. User can **unmap** the transaction groups by selecting accounts and then clicking on Save button to reset their mapping with Group Corporate
16. User can click on **Delete Party Mapping** to delete all the transaction and party account access maintenance done for corporate party in one step.
17. User can drill down his search by applying Filter to search an account basis on Transaction Group, currency, mapping status
18. **Click Save** to save the maintenance, and redirect to the review page.
    OR
    Click **Next** to proceed to the next logical step.
    OR
    Click **Submit** to submit the steps performed so far for approval.
    OR
    Click **Retain Draft** to save the details entered as draft.
    OR
    Click **Cancel** to cancel the transaction.

Note: Admin can submit the maintenance after any step. Maintenances saved so far will be sent for approval in one flow. Admin would not be able to make any changes or maintain another step for the same Group Corporate till the time the approval of the wizard is not done.

19. The **Review** screen appears. Verify the details, and click **Submit**.
    OR
    Click **Edit** to modify the details entered.
    OR
    Click **Next** to proceed to next step.
    OR
    Click **Retain Draft** to save all the steps completed so far, and allow Admin resume the same application.
    OR
    Click **Cancel** to cancel the transaction.
20. The success message appears along with the transaction reference number

Note: Following flow explains the Drill down options to search by applying Filter to search an account for Virtual Accounts Management & Liquidity Management module –

Virtual Account Management (Real Account) Tab-



To view Virtual Account Management - Real Accounts:

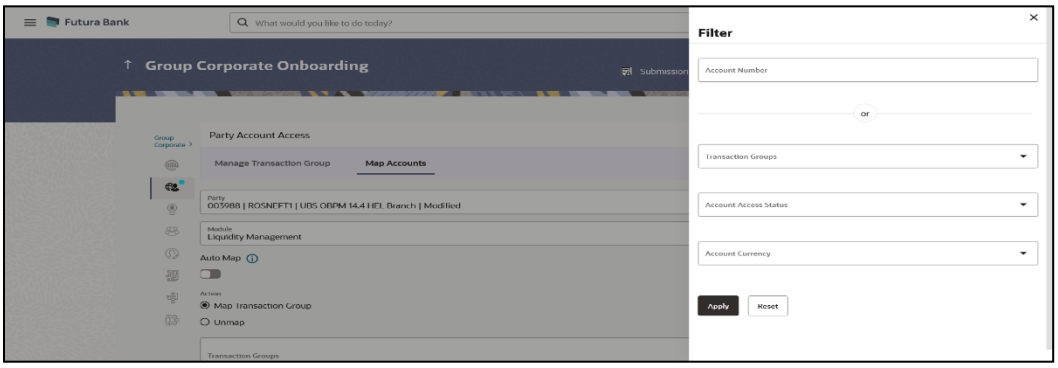
1. In the **Account Number** field, enter the exact Real Account number.
   OR
   From the **Branch name** drop down, select the Branch name.
   OR
   From the **Transaction groups**, select the transaction group.
   OR
   From the **Account Access Status** field, select an appropriate status.
   OR
   From the **Currency** field, select the required currency .
2. Click **Apply** to Apply the filter.
   OR
   Click **Reset** to reset the entered data.
3. The user can filter through two sections :

   1. On the basis of the Account Number.

   OR

   2. A combination of branch name, currency filters and other parameters . After the OR division, the user can use these search parameters alone or in a combination to filter search results.

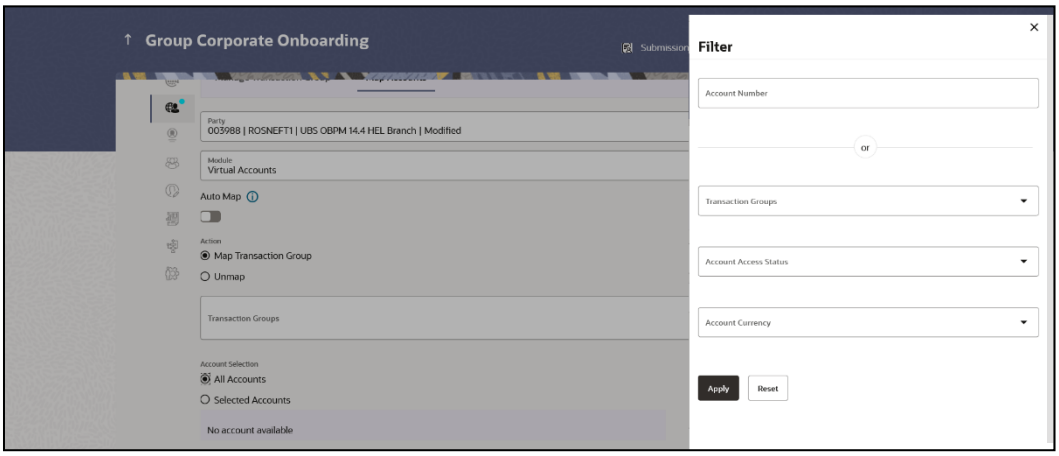
Liquidity Management Tab -



To view Liquidity Management Accounts:

1. In the **Account Number** field, enter the exact Real Account number.
   OR
   From the **Branch name** drop down, select the Branch name.
   OR
   From the **Transaction groups**, select the transaction group.
   OR
   From the **Account Access Status** field, select an appropriate status.
   OR
   From the **Currency** field, select the required currency
2. Click **Apply** to Apply the filter.
   OR
   Click **Reset** to reset the entered data.
3. The user can filter through two sections :
   1. On the basis of the Account Number.
      OR
   2. A combination of branch name, currency filters and other parameters . After the OR division, the user can use these search parameters alone or in a combination to filter search results.

Virtual Accounts Tab -



To view Virtual Accounts:

1. In the **Virtual Account Number** field, enter the exact Virtual Account number.
   OR
   In the **Virtual Account Name** field, enter the Virtual Account Name.
   OR
   From the **Virtual Entity** search, select the Virtual Entity name.
   OR
   From the **Branch name** drop down, select the Branch name.
   OR
   From the **Transaction groups**, select the transaction group.
   OR
   From the **Account Access Status** field, select an appropriate status.

OR
From the **Status** drop down, select the status.
OR
From the **Currency** field, select the required currency

2. Click **Apply** to Apply the filter.
   OR
   Click **Reset** to reset the entered data.
3. The user can filter through two sections :

   1. On the basis of the Account Number
   OR

   2. A combination of branch name, currency filters and other parameters . After the OR division, the user can use these search parameters alone or in a combination to filter search results .

15.3.4 Party Account Access- Delete

As part of this option, party account mapping can be deleted.

To delete account and transaction access for the party:

9. From the **Mapping Summary of Party** dropdown list, select the corporate party id.
10. For a searched party, summary screen will be displayed with total accounts associated with corporate party, status of the accounts mapped for the internet banking, modified accounts if any and Auto account mapping status .
11. Click the link under the total **Mapped accounts** or **Modified accounts**, The **Party Account Access – View** (Transaction Mapping) screen appears. . The search result according to the search criteria appears
    OR
    All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories
12. Click **Map** or **Edit** (available across each banking module). The **Party Account Access - Edit** screen appears.
    OR
    Click **Cancel** to cancel the transaction.
13. Click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate party in one-step.

    The application prompt the administrator with a message Are you sure you want to delete Party Account Access setup for linked Party ID – Party name with an option of Yes / No.
14. Click **Yes** to proceed with the deletion request.
    It will navigate to confirmation page with a success message and the status.
    OR
    Click **No** if you do not wish to proceed with deletion.
15. Click **OK** to complete the transaction.

16. **Click Save** to save the maintenance, and redirect to the review page.
    OR
    Click **Next** to proceed to the next logical step.
    OR
    Click **Submit** to submit the steps performed so far for approval.
    OR
    Click **Retain Draft** to save the details entered as draft.
    OR
    Click **Cancel** to cancel the transaction.
17. The **Review** screen appears. Verify the details, and click **Submit**.
    OR
    Click **Edit** to modify the details entered.
    OR
    Click **Next** to proceed to next step.
    OR
    Click **Retain Draft** to save all the steps completed so far, and allow Admin resume the same application.
    OR
    Click **Cancel** to cancel the transaction
18. The success message appears along with the transaction reference number

15.4 Step 3: User Onboarding

Using this step user(s) is onboarded under a Group Corporate. This function allow system/ bank administrator to create a new user from scratch or by copying an existing user.

User Management function enables System/ Bank Administrator to onboard and manage users and their login credentials for channel banking access.

This function also lets the System/Bank Administrator to define the various touch points from which the user can access the channel banking and limit package applicable for the same.

In a multi entity scenario, this function enables system/ bank administrator to provide access to multiple entities to users.

When Corporate User switches to an accessible entity, the roles associated with the new entity are applicable, allowing the user to perform transactions specific to the switched entity (accessible entity).

Roles mapped to the specific entity shall be available for mapping it to the users

---

Note:
• User is created first in IDCS and then onboard in OBDX.
• When an administrator creates/modifies a user through User Management either via Group Corporate onboarding (for corporate user) or via standalone screens (for administrator and retail user), the global roles would be available for assignment to the user in the same manner as is available in the current system, however, the entity specific roles would be listed in Entity-specific sections for each user. Administrator will be able to map multiple roles to the user under each entity

---

The user details also shows the list all the user groups associated with a particular user. In order to remove a particular user from a user group, the administrator must manually go to the particular user group screen and remove the user.

A DND (do not disturb) flag is also enabled at User Onboarding level. It allows System/ Bank Administrator to enable/disable Do not disturb (DND) Flag for Mandatory Alerts. User will not receive any alerts for the transactions marked as DND. User will receive the alerts only after performing any transactions of respective category post removing DND flag.

Internal Users

- System Administrator
- Bank Administrator

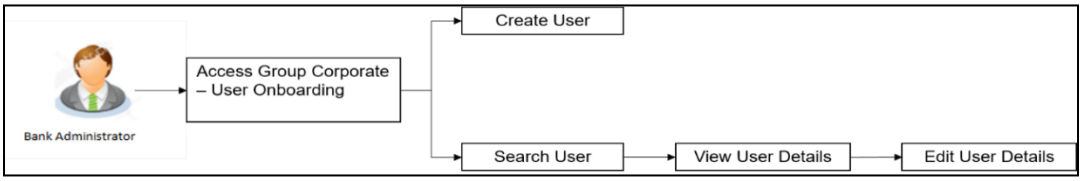
External Users

- Corporate User
- Corporate Administrator

Pre-Requisites

- User Segment and Application roles are maintained
- Transactions are associated with each Application role
- Transaction (User Management) access is provided to System/Bank Administrator.
- Approval rule set up for Bank administrator to perform the actions.
- Party Preference is maintained for corporate user

Workflow



How to reach here:

System/ Bank Administrator Dashboard > Corporate Onboarding > Group Corporate Onboarding > User Onboarding tab
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Group Corporate Onboarding > User Onboarding tab

15.4.1 User Management - Search and View

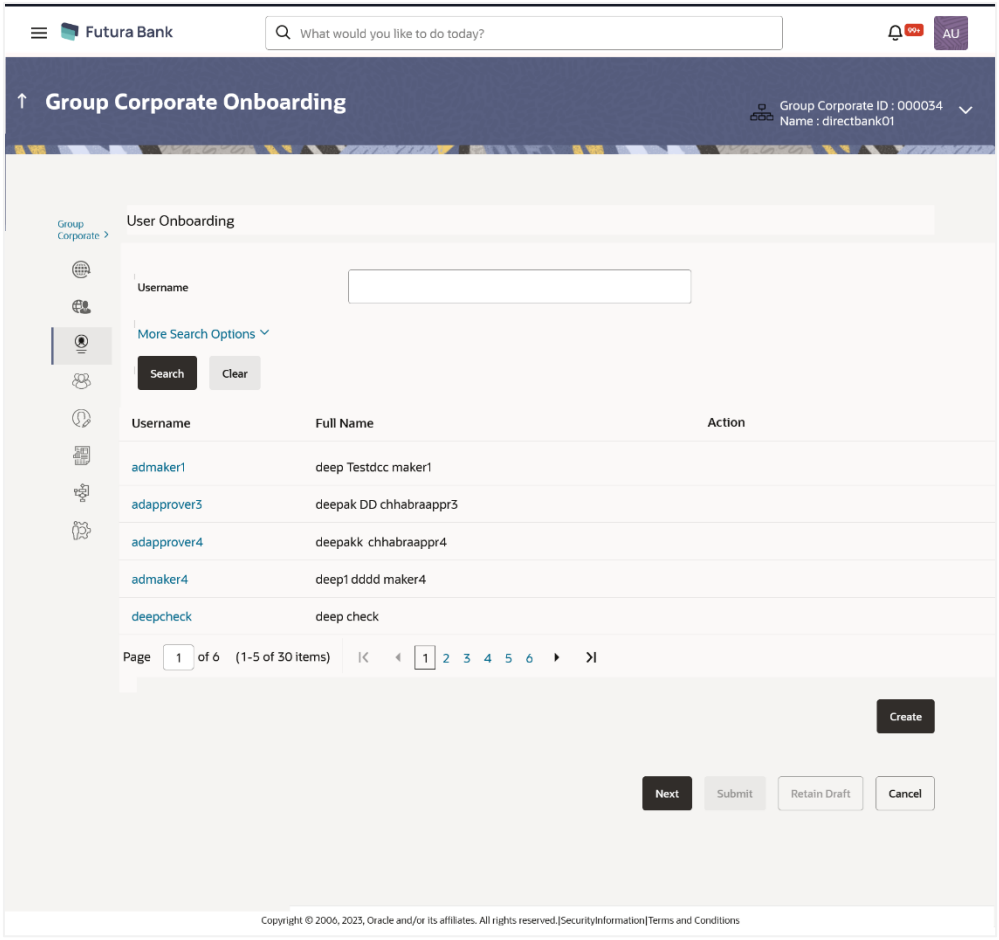
Using this option, System/ bank administrators can search and view details of the existing users.

Default search is available with User Name, but the user can also be searched by providing other details like First Name, Last Name, Party ID. Email ID and Mobile Number.

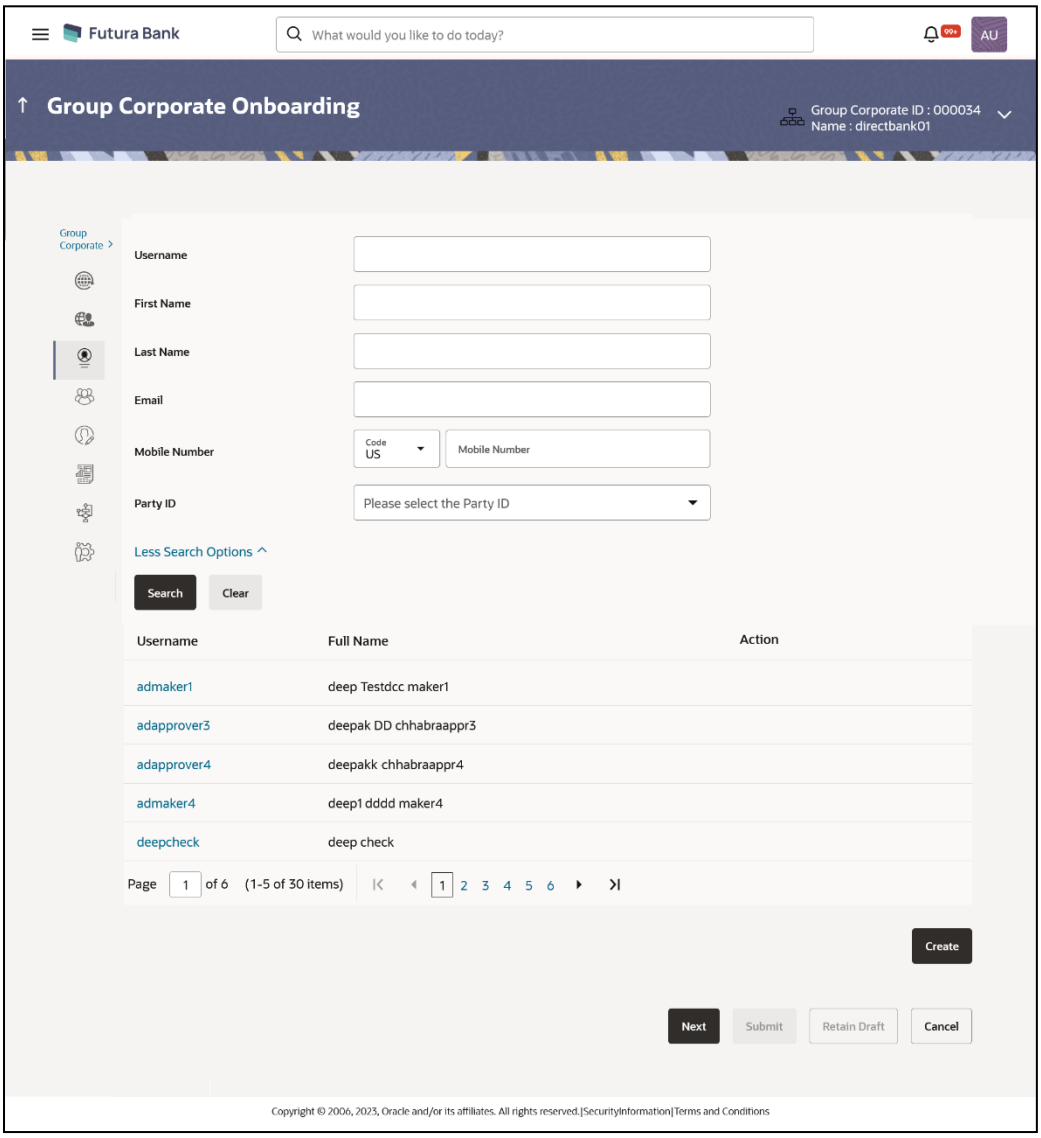
To search for a user:

1. Enter the search criteria, click **Search**.
   The search results appear on the **User Management** screen based on the search parameters.
   OR
   Click **Cancel** if you want to cancel the transaction.
   OR
   Click **Clear** if you want to reset the search parameters.
   OR
   Click **Create** to create the to create internal and external users.

User Management - Search



User Management - More Search Options



Field Description

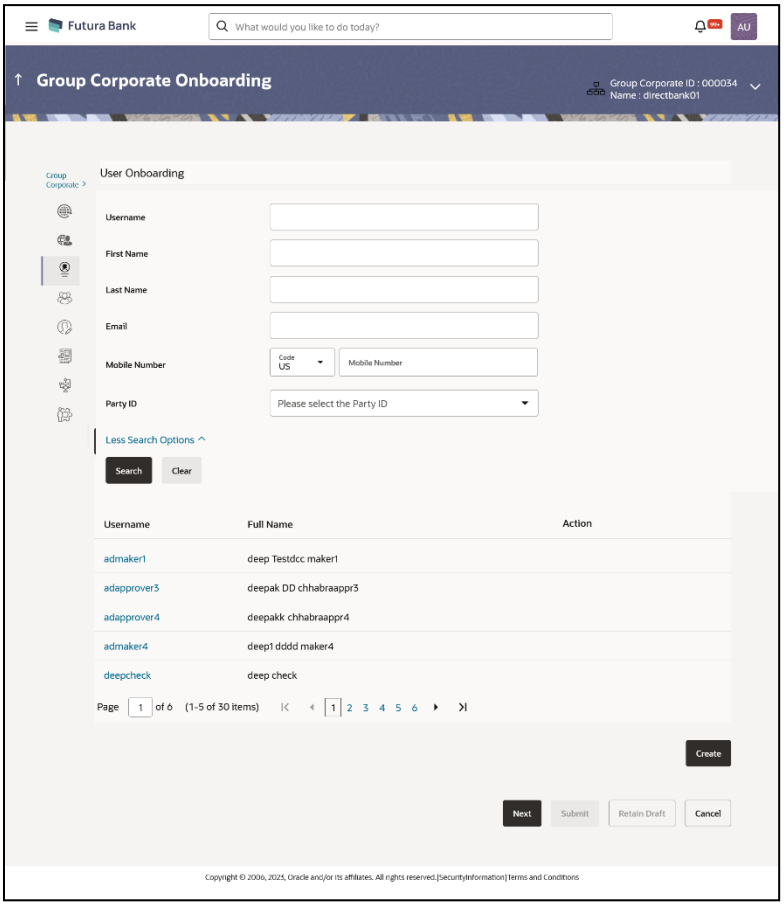
Field Name	Description
User Name	To search the user with the user name. Partial search is allowed.
More Search Options	
Below fields appears if you click the **More Search Options** link.	
First Name	Allows to search based on first name or given name of the user.

Field Name	Description
Last Name	Allows to search based on last name/ surname of the user.
Email	Allows to search based on email id of the user.
Mobile Number	Allows to search based on mobile number of the user. Note: Select international subscriber dialing (ISD) code along with the mobile number to search the user.
Party ID	Allows to search based on Party id.

To view the user details:

1. Enter the search criteria and click **Search** in the User Management screen. The search results appear based on the search parameters.

User Management - Search Results



Field Description

Field Name	Description
Search Results	
User Name	User Name of the user.
Full Name	First name and last name of the user.
Action	Status of the user.

2. Click the **User Name** link of the record for which you want to view the user details. The **User Management - View** screen appears.

User Management – View

Field Description

Field Name	Description
View	
User Type	Type of user. The user will be: • Corporate User
Group Corporate ID	Group Corporate ID mapped to the user is displayed.
Party ID	Party ID for which the user is created will be displayed.
Personal Information	
User Name	Name of the user (login ID) of the user.
Title	Title of the user. The options are: • Mr • Mrs • Miss • Ms • Dr • Master
First Name	First name of the user.
Middle Name	Middle name of the user.
Last Name	Last name/ surname of the user.
Date of Birth	Date of birth of the user.
Contact Details	
Email ID	Email id of the user.
Contact Number (Mobile)	The mobile number of the user alongwith an international subscriber dialing (ISD) code.

Contact Number (Land Line)	Phone number (land line) number of the user.
Address Line 1-4	Address of the user.
Country	Country of the user.
City	City in which the user resides.
Zip Code	The postal code of the city in which the user resided.

User Groups And Global Roles

User Groups	The list of all user groups to which the selected user belongs. Note: • This information is read-only and hence cannot be modified. • If a particular user needs to be removed from a user group, then the administrator must manually go to the particular user group screen and remove the user.
Roles	The global roles which are mapped to the users.
Is Corporate Administrator	Displays whether the corporate user is corporate administrator or not.

DND Alerts

DND Alerts	The list of categories for which DND is configured can be enabled or disabled using this option.

Device Registration

Android Devices	This option shows if the user has registered futura Bank application on any android devices/s. Enabling of the device happens when the user installs and registers on the app on the android device. Administrator cannot manually enable the device. If the Administrator deregisters the device, the user gets logged out from all the android devices and his alternate login gets disabled from all the android devices on which the user has installed the application.

iOS Devices

This option shows if the user has registered futura Bank application on any iOS devices/s. Enabling of the device happens when the user installs and registers on the app on the iOS device. Administrator cannot manually enable the device.

If the Administrator deregisters the device, the user gets logged out from all the iOS devices and his alternate login gets disabled from all the iOS devices on which the user has installed the application.

Push Notifications

Android Devices

This option shows if the user has registered for push notifications for android devices. Enabling of the push notification is done by user himself and administrator cannot do the same.

If the administrator disables this, the user will stop getting notifications as a pop-up message (push notification) on the user's registered mobile number.

iOS Devices

This option shows if the user has registered for push notifications for iOS devices. Enabling of the push notification is done by user himself and administrator cannot do the same.

If the administrator disables this, the user will stop getting notifications as a pop-up message (push notification) on the user's registered mobile number.

Note: To receive push notification user will have to allow the same on the device settings.

Primary Entity Details

Entity Name

Primary Entity name associated to the user.

Map Parties

Primary Party

Primary Entity name associated to the user.

Accessible Parties

Accessible Entities associated to the user.

Limits

Limits attached to the user.

Touch Points

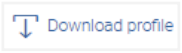
Name of touch points/ groups maintained under a specific entity for which the limit packages are mapped.

Map Roles

Displays the roles to which the entities are mapped.

Accessible Entity Details

Entity Name	Accessible Entity name associated to the user.
Map parties	
Primary Party	Primary Party ID details of the user is associated with the New Entity
Accessible Parties	Accessible Party Details that user has access.
Limits	Limits package associated to the user for the accessible entity.
Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for which the limit packages are mapped.
Map Role	The roles to which the entities are mapped.

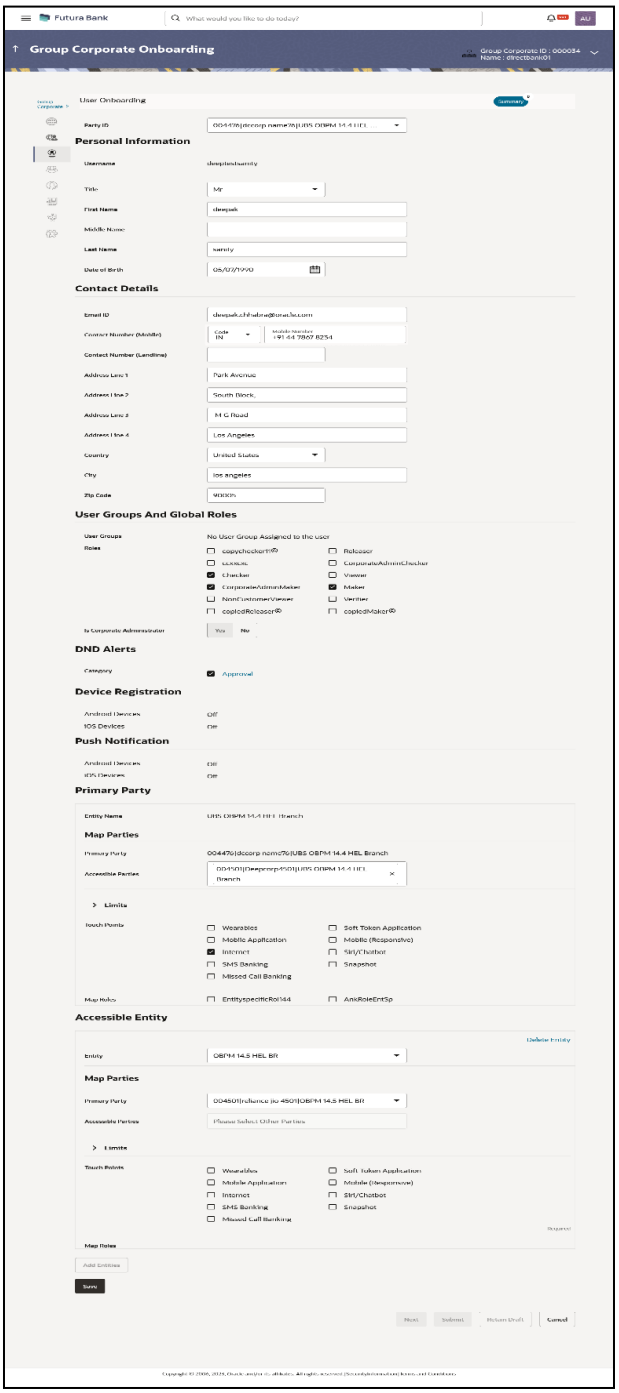
3. Click **Edit** to edit the user details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click 

   to download the user details.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.

15.4.2 User Management - Edit

This function enables the Administrator to edit the existing user details.

User Management – Edit



Field Description

Field Name	Description
Edit	
Party ID	Party ID for which the user is created will be displayed. This is editable field.
Personal Information	
User Name	Name of the user (login ID) of the user.
Title	Title of the user. This is editable field. The options are: • Mr • Mrs • Miss • Ms • Dr • Master
First Name	First name of the user. This is editable field.
Middle Name	Middle name of the user. This is editable field.
Last Name	Last name/ surname of the user. This is editable field.
Date of Birth	Date of birth of the user. This is editable field.
Contact Details	
Email ID	Email id of the user. This is editable field.

Business Contact Number (Mobile)

The contact number of the user alongwith an international subscriber dialing (ISD) code.

Contact Number (Mobile)

The mobile number of the user alongwith an international subscriber dialing (ISD) code.

If user type is Retail & Business , value is fetched from the core banking application and defaulted. This is editable field.

Note: The mobile number field allow to capture the correct number of digits based on the selected country code.

Contact Number (Land Line)

Phone number (land line) number of the user.

This is editable field.

Address Line 1-4

Address of the user.

This is editable field.

Country

Country of the user.

This is editable field.

City

City in which the user resides.

This is editable field.

Zip Code

The postal code of the city in which the user resided.

This is editable field.

Roles

Application roles mapped to the user.

In case of multi entity setup, these roles will be for the default/home entity of the user.

This is editable field.

User Groups And Global Roles

User Groups

The list of all user groups to which the selected user belongs.

This is editable field.

Note:
• This information is read-only and hence cannot be modified.
• If a particular user needs to be removed from a user group, then the administrator must manually go to the particular user group screen and remove the user.

Roles	The global roles which are available for mapping it to the users. This is editable field.
Is Corporate Administrator	Define whether the corporate user is corporate administrator or not. This is editable field.

DND Alerts

Category	The categories for which DND (do not disturb) needs to be enabled. All the categories for which DND is applicable are listed for selection. This is editable field.

Device Registration

This is non editable section.

Android Devices	This option shows if the user has registered futura Bank application on any android devices/s. Enabling of the device happens when the user installs and registers on the app on the android device. Administrator cannot manually enable the device. If the Administrator deregisters the device, the user gets logged out from all the android devices and his alternate login gets disabled from all the android devices on which the user has installed the application.
iOS Devices	This option shows if the user has registered futura Bank application on any iOS devices/s. Enabling of the device happens when the user installs and registers on the app on the iOS device. Administrator cannot manually enable the device. If the Administrator deregisters the device, the user gets logged out from all the iOS devices and his alternate login gets disabled from all the iOS devices on which the user has installed the application.

Push Notifications

This is non editable section.

Android Devices

This option shows if the user has registered for push notifications for android devices. Enabling of the push notification is done by user himself and administrator cannot do the same.

If the administrator disables this, the user will stop getting notifications as a pop-up message (push notification) on the user's registered mobile number.

iOS Devices

This option shows if the user has registered for push notifications for iOS devices. Enabling of the push notification is done by user himself and administrator cannot do the same.

If the administrator disables this, the user will stop getting notifications as a pop-up message (push notification) on the user's registered mobile number.

Note: To receive push notification user will have to allow the same on the device settings.

Primary Entity Details

Entity Name

Primary Entity name associated to the user.

Map Parties

Primary Party

Primary Entity name associated to the user.

Accessible Parties

Accessible Entities associated to the user.

This is editable field.

Limits

Limits attached to the user.

Touch Points

Name of touch points/ groups maintained under a specific entity for which the limit packages are mapped.

This section is editable.

Map Roles

Displays the roles to which the entities are mapped.

This section is editable.

Accessible Entity Details

Entity

Accessible Entity name associated to the user.

This is editable field.

Map Parties

Primary Party	Primary Party ID details of the user is associated with the New Entity. This is editable field.
Accessible Parties	Accessible Party Details that user has access.
Limits	Limits package associated to the user for the accessible entity.
Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for which the limit packages are mapped. This section is editable.
Map Role	The roles to which the entities are mapped.

To edit or update a user details:

1. Enter the search criteria, click **Search**.
   The **search** results appear on the **User Management** screen based on the search parameters.
   OR
   Click **Clear** if you want to reset the search parameters.
   OR
   Click **Cancel** if you want to cancel the transaction.
2. In the **User Management - Search Results** section, click the **User Name** link of the record for which you want to edit the user details.
   The **User Management - View** screen appears.
3. Click **Edit** to update the user information.
4. From the **Party ID** list, select the Party ID for which the user is created.
5. In the **Personal Information** section, enter the required details.
6. In the **Contact Details** section, enter the required details.
7. In the **User Groups and Global Roles** section, select the checkbox (s) against the **Roles** field to map roles to the user.
8. In the **Is Corporate Administrator** field, select the appropriate option to define whether the corporate user is corporate administrator or not.
9. In the **Category** field, select the checkbox(es) categories for which DND (do not disturb) needs to be enabled.
10. In the **Accessible Entity Details** section, add the accessible entities for the user.
11. In the **Limits** section,
    a. In the **Touch Points** section, select the touch points to be mapped to user.
    b. Select the appropriate limit package under the **Package** for each touch point column.
    c. In the **Map Roles** field, select the checkbox(es) adjacent to roles to which the entities are to be mapped.

12. In the **Accessible Entity** section, add the accessible entities for the user and select the party and limits for that entity (applicable only if Bank has Multi Entity setup).

    a. In the **Primary Party ID** field, select the Primary Party ID mapped to the user which is associated with the New Entity

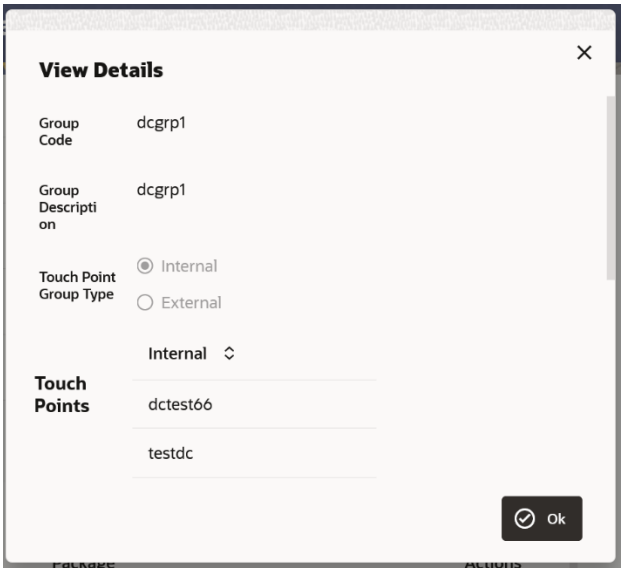
    d. In the **Limits** section, select the appropriate limit package under the Package for each touch point column.

    e. In the **Touch Points** section, select the touch points to be mapped to user.

    f. Select the appropriate limit package under the **Package** for each touch point column.

    b. In the **Map Roles** field, select the checkbox(es) adjacent to roles to which the entities are to be mapped.

Touch Points Group - View Details



Field Description

Field Name	Description
Group Code	Group code defined for touch point group.
Group Description	Group description defined for touch point groups.
Group Type	Type of touch point i.e. whether touch point is of type internal or external.
Touch Points	List of the internal or external touch points.

13. **Click Save** to save the maintenance, and redirect to the review page.
    OR

Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate to the previous screen.
OR
Click **Next** to proceed to the next logical step.
OR
Click **Submit** to submit the steps performed so far for approval.
OR
Click **Retain Draft** to save the details entered as draft.
OR
Click **Cancel** to cancel the transaction.

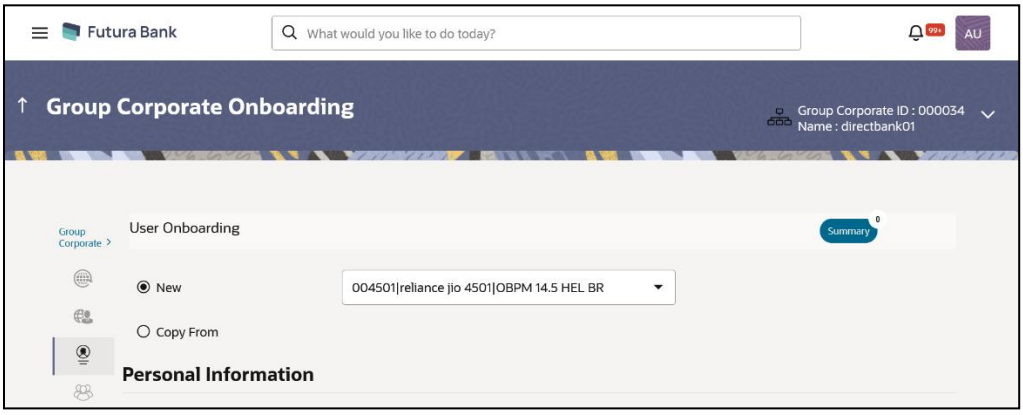
14. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate back to previous screen.
15. The success message of updates appears.

15.4.3 User Management - Create

System/Bank Administrator logs into the system and navigates to the User Management screen. This function allows the administrator to create internal and external users.

Note: In case of multi entity implementation, if the system/bank administrator has access to multiple entities, then the administrator can select the entity from the entity switcher on which the user needs to be onboarded. The selected entity of the user as part of onboarding will be the default/home entity of the user being created.

Group corporate Onboarding - *User Onboarding*



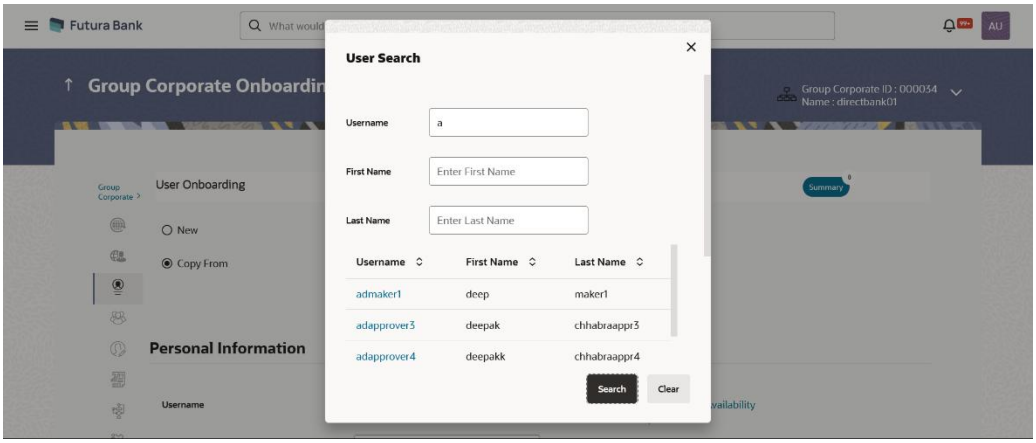
Field Description

Field Name	Description
New	Allows selecting a Parent Party ID of the user.
Copy From	Allows to select an already created user (user created under the same Group Corporate) and screen will display the copied data for all the sections except Personal and Contact information. System/ Bank Administrator would require to fill Personal and Contact information and he can make the changes in the copied data as well.
Party ID	Parent Party ID of the user for mapping it to the user.

To onboard a user:

1. In the **User Management** screen, Click **Create**.
2. Select the option to create a new or by copying an existing user.
3. If you select **New** option;
   a. From the **Party ID** list, select a Parent Party ID of the user.
   The **Personal Information, Contact Details, Touch Points, Roles, Limits** and **Accessible Entity** sections appear.
4. If you select the **Copy From** option;
   a. The **User Search** popup window appears.
   b. Enter the search criteria, and click **Search**.
   The search results appear on the **Search User** screen based on the search parameters.
   OR
   Click **Clear** if you want to reset the search parameters.

User Management – User Search

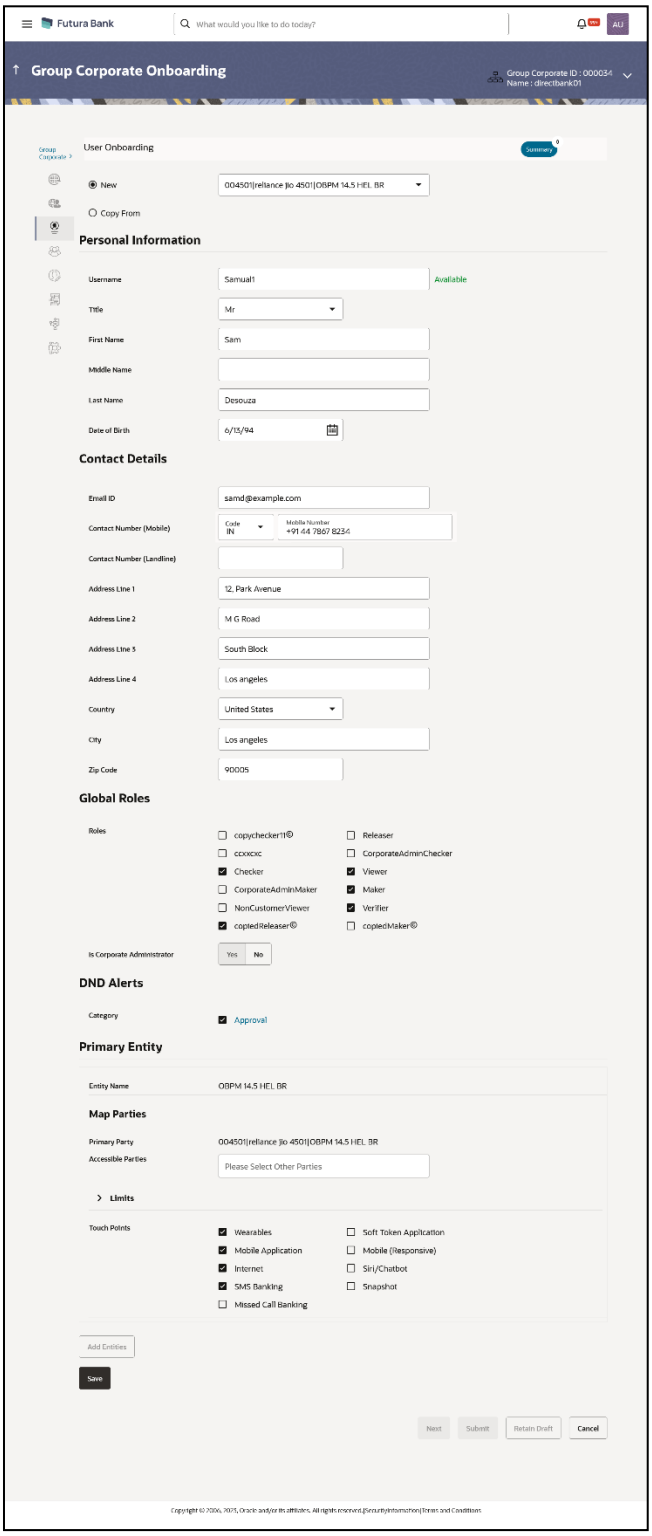


Field Description

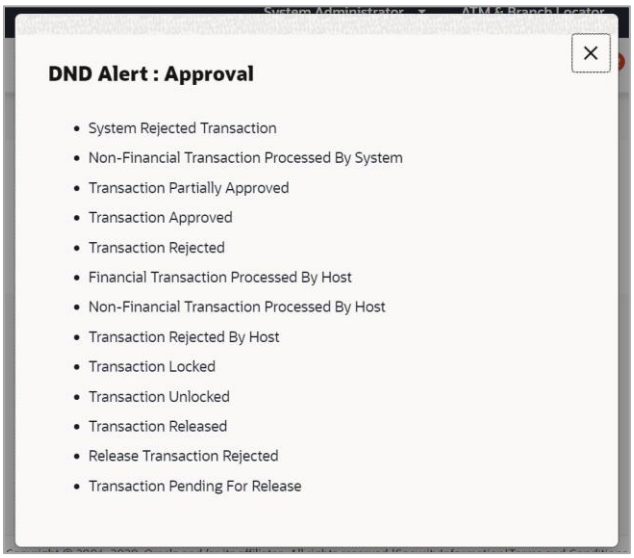
Field Name	Description
Search	
User Name	To search the user with the user name. Partial search is allowed.
First Name	Allows to search based on first name or given name of the user.
Last Name	Allows to search based on last name/ surname of the user.
Search Results	
User ID	User ID of the user.
First Name	First Name of the user.
Last Name	Last Name of the user.

c. Click the **User ID** link of the record for which you want to onboard.
The **Personal Information, Contact Details, Touch Points, Roles, Limits** and **Accessible Entity** sections appear.

User Onboarding



DND Alerts - Category Details



Field Description

Field Name	Description
Create	
Personal Information	
User Name	Name of the user (login ID) of the user.
Title	Title of the user. The options are: • Mr • Mrs • Miss • Ms • Dr • Master
First Name	First name of the user.
Middle Name	Middle name of the user.
Last Name	Last name/ surname of the user.

Field Name	Description
Date of Birth	Date of birth of the user.
Contact Details	
Email ID	Email id of the user.
Business Contact Number (Mobile)	The contact number of the user alongwith an international subscriber dialing (ISD) code. If user type is Retail and Business User, value is fetched from the core banking application and defaulted. Note: The mobile number field allow to capture the correct number of digits based on the selected country code.
Contact Number (Mobile)	The mobile number of the user alongwith an international subscriber dialing (ISD) code. If user type is Retail & Business , value is fetched from the core banking application and defaulted.
Contact Number (Land Line)	Phone number (land line) number of the user.
Address Line 1-4	Address of the user.
Country	Country of the user.
City	City in which the user resides.
Zip Code	The postal code of the city in which the user resided.
Roles	Application roles mapped to the user. In case of multi entity setup, these roles will be for the default/home entity of the user.
Global Roles	
Roles	The global roles which are available for mapping it to the users.
Is Corporate Administrator	Define whether the corporate user is corporate administrator or not.

Field Name	Description
Touch Points	
Selected Touch Points	The touch points (banking channels) selected for a user to perform transactions. The touch points could be: • Mobile Application • Mobile (Responsive) • Internet • Missed Call Banking • SMS Banking • Wearables • Snapshot • Siri / Chatbot • API Access • Soft Token Application
DND Alerts	
Category	The categories for which DND needs to be enabled. All the categories for which DND is applicable are available for selection. Note: Click on category link to view list of all the events for which alerts will not be sent to the user.
Primary Entity	
Entity Name	Primary Entity name associated to the user.
Map Parties	
Primary Party	Primary party name associated to the user.
Accessible Parties	Accessible Party Details that user has access.
Limits Limits attached to the user.	

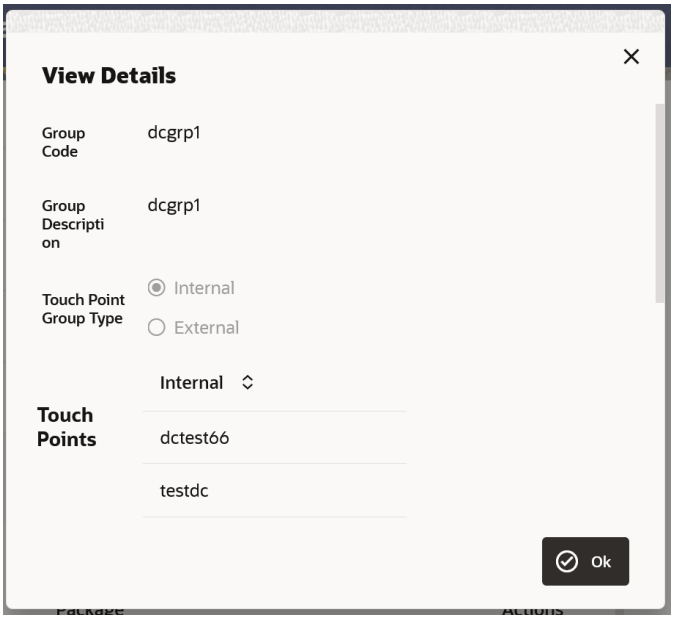
Field Name	Description
Touch Points/ Group	Name of touch points/ groups maintained under a specific entity for which the limit packages are mapped.
Package	Name of the limit package mapped against specific touch points /touch point groups.
Touch Points	The touch points (banking channels) selected for a user to perform transactions. The touch points could be: • Mobile Application • Mobile (Responsive) • Internet • Missed Call Banking • SMS Banking • Wearables • Snapshot • Siri / Chatbot • API Access • Soft Token Application
Map Roles	The roles to which the entities are mapped.
Accessible Entity Details	
Entity	Accessible Entity name associated to the user.
Map Parties	
Primary Party	Primary Party ID details of the user is associated with the New Entity.
Accessible Parties	Accessible Party Details that user has access.
Limits	
Limits package associated to the user for the accessible entity.	
Touch Points	The touch points (banking channels) selected for a user to perform transactions.

Field Name	Description
Package	Name of the limit package mapped against specific touch points /touch point groups.
Map Role	The roles to which the entities are mapped.

5. In the **User Name** field, enter the required details. Click **Check Availability** to check the uniqueness of the user ID. If the user ID is already used, then enter a unique valid username.
6. In the rest of the **Personal Information** section, enter the required details.
7. In the **Contact Details** section, enter the required details.
8. In the **Global Roles** section, select the checkbox (s) against the **Roles** field to map roles to the user.
9. In the **Is Corporate Administrator** field, select the appropriate option to define whether the corporate user is corporate administrator or not.
10. In the **Category** field, select the checkbox(es) categories for which DND (do not disturb) needs to be enabled.
11. In the **Accessible Parties** field in the **Map Parties** section, select the parties to map with user.
12. In the **Limits** section,
    a. In the **Touch Points** section, select the touch points to be mapped to user.
    b. Select the appropriate limit package under the **Package** for each touch point column.
    c. In the **Map Roles** field, select the checkbox(es) adjacent to roles to which the entities are to be mapped.
13. In the **Accessible Entity** section, add the accessible entities for the user and select the party and limits for that entity (applicable only if Bank has Multi Entity setup).
    c. In the **Primary Party ID** field, select the Primary Party ID mapped to the user which is associated with the New Entity
    d. In the **Limits** section, select the appropriate limit package under the Package for each touch point column.
    e. In the **Touch Points** section, select the touch points to be mapped to user.
    f. Select the appropriate limit package under the **Package** for each touch point column.
    d. In the **Map Roles** field, select the checkbox(es) adjacent to roles to which the entities are to be mapped.
    e. Click **Add Entities** button, to add accessible entity to a user.
    a.

Touch Points Group - View Details

This pop-up screen appears on clicking beside a touch point group in the **Limits** section, which appears when onboarding corporate user types.



Field Description

Field Name	Description
Group Code	Group code defined for touch point group.
Group Description	Group description defined for touch point groups.
Group Type	Type of touch point i.e. whether touch point is of type internal or external.
Touch Points	List of the internal or external touch points.

14. **Click Save** to save the maintenance, and redirect to the review page.
    OR
    Click **Next** to proceed to the next logical step.
    OR
    Click **Submit** to submit the steps performed so far for approval.
    OR
    Click **Retain Draft** to save the details entered as draft.
    OR
    Click **Cancel** to cancel the transaction.

Note: Admin can submit the maintenance after any step. Maintenances saved so far will be sent for approval in one flow. Admin would not be able to make any changes or maintain another step for the same Group Corporate till the time the approval of the wizard is not done.

15. The **Review** screen appears. Verify the details, and click **Submit**.
    OR
    Click **Add Another** to add another maintenance of the same step.
    OR
    Click **Edit** to modify the details entered.
    OR
    Click **Next** to proceed to next step.
    OR
    Click **Retain Draft** to save all the steps completed so far, and allow Admin resume the same application.
    OR
    Click **Cancel** to cancel the transaction.
16. The success message of user creation appears along with the transaction reference number.

15.5 Step 4: User Group Maintenance

User group is a set of x users with similar interests and goals.

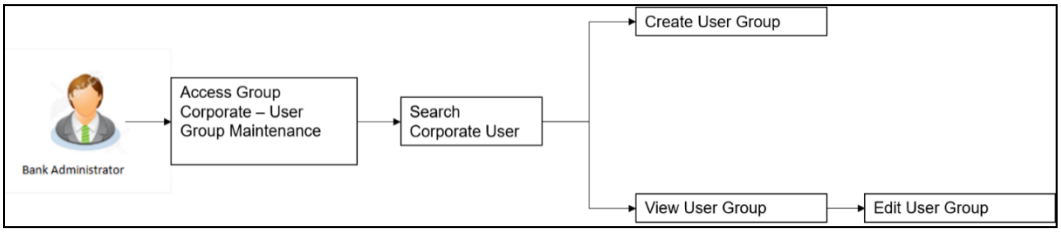
Using User Group maintenance option Bank administrator can maintain the user groups of corporate users of Group corporate irrespective of Corporate Party. User Groups will be created at the Group Corporate level.

User groups maintained by administrators for corporate users are used while creating approval workflows and approval rules.

Prerequisites:

- Transaction access is provided to Bank Administrator.
- Multiple corporate users are maintained.
- Approval rule set up for Bank administrator to perform the actions.
- Party preference for which the groups are to be created is maintained and is active.

Workflow



Features Supported In Application

User Group Management allows Bank Administrator to:

- Create User Groups
- View User Groups
- Modify User Groups

How to reach here:

System/ Bank Administrator Dashboard > Corporate Onboarding > Group Corporate Onboarding > User Group
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Group Corporate Onboarding > User Group

15.5.1 User Groups – Create

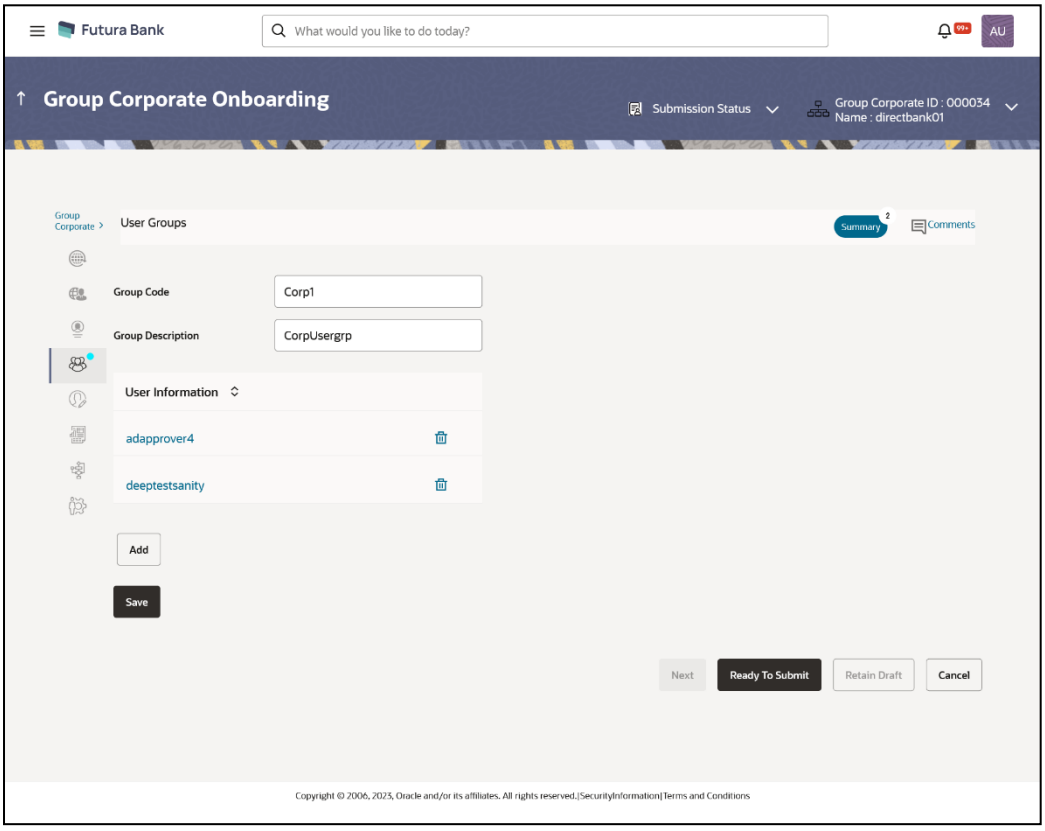
Bank Administrator can create a new User Group for the Group Corporate ID by using this option. Only the users of single Group Corporate ID can be clubbed together in a User Group.

Administrator can create multiple user groups and one user can be part of multiple user groups. Bank Administrator will be allowed to create user group even without adding a single user.

To create a user group:

1. The **User selection** screen appears. Select the appropriate option.

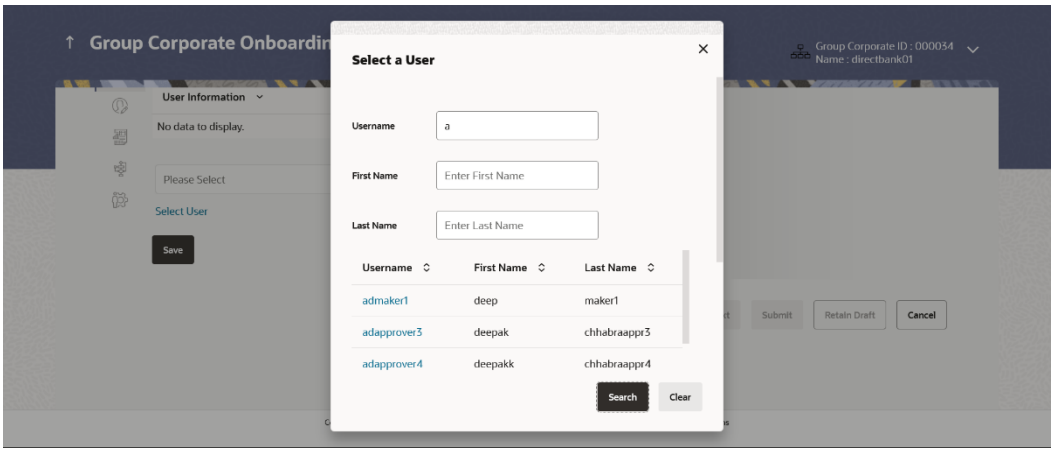
User Group - Create



Field Description

Field Name	Description
Group Code	To specify User Group code.
Group Description	To specify User Group description.
User Information	Search and select user to map with User Group which is being created

Search User



Field Description

Field Name	Description
Search User	
Username	Search User by using Username to map with user group
First Name	Search and select user by using First name and add a user to the user group. Users belonging to the same Group Corporate will be listed.
Last Name	Search and select user by using Last name and add a user to the user group. Users belonging to the same Group Corporate will be listed.
Search Result	
Username	Display username of the searched user
First Name	Display First name of the searched user
Last Name	Display Last name of the searched user

2. Click **Create**.
3. In the **Group Code** field, enter the group code.
4. In the **Group Description** field, enter the group name.

5. In the **User Group** section, Click **Add** to add the selected user in the User Group.
   Click on the **Select User** link, the **Select User** popup appears.
   Search the user by adding search criteria, and click **Search**.
   Based on search criteria, search result appears.
   Click on the user which to be added, and click **Add** to add to table.

Note: Once added, the user name will be removed from the user drop-down to avoid duplication of users. Click to remove a user from the User Group.

6. Click **Save** to save the maintenance, and redirect to the review page.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.

Note: Admin can submit the maintenance after any step. Maintenances saved so far will be sent for approval in one flow. Admin would not be able to make any changes or maintain another step for the same Group Corporate till the time the approval of the wizard is not done.

Click **Add Another** to add new user group in same flow.
OR
Click **Edit** to modify the details entered.
OR
Click **Next** to proceed to next step.
OR
Click **Retain Draft** to save all the steps completed so far, and allow Admin resume the same application.
OR
Click **Cancel** to cancel the transaction.

15.5.2 User Groups – Summary & View

Once the logged in Bank Administrator navigates to User Group Management screen, and searches User Group Code. User groups maintained if any under the Group Corporate would be displayed on the screen. User can opt to view the details of existing user groups.

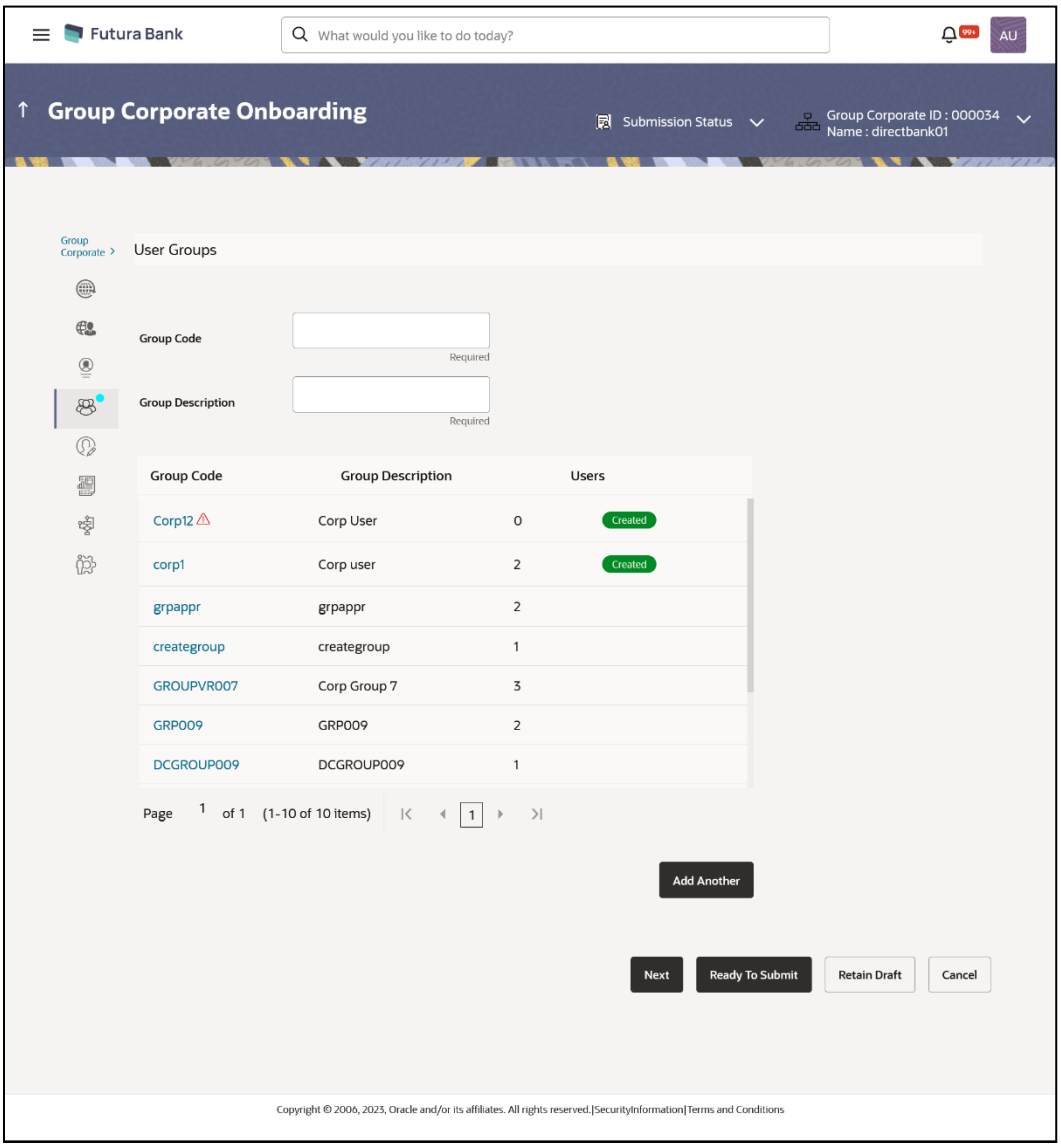
The summarized view of all the user groups created (if any) for the Group corporate is displayed on the screen. Further drill down is given on each user group to view the details of the users who are part of the user group.

To search and view User Group details of the Group Corporate:

1. In **User Group Management** screen, in the **Group Code** or in **Group Description** enter the respective details.

2. Click **Search**. User groups maintained if any under the Group Code or Group Description are displayed on the screen.

Summary screen

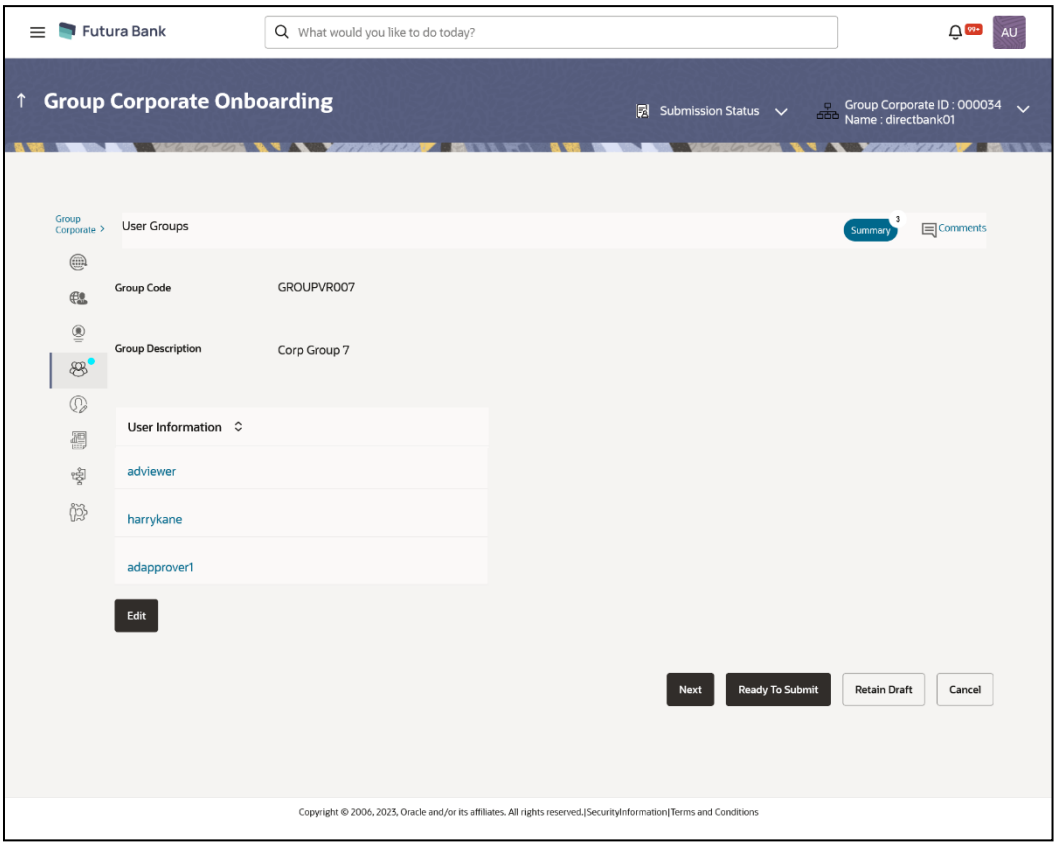


Field Name	Description
Search User Group	
Group Code	Enter User group code
Group Description	Enter Description provided to the user group.

Field Name	Description
Search Result	
Group Code	Display user group code
Group Description	Display description provided to the user group
User Count	Display Number of users available in each user group

3. Click on **Group Code** hyperlink to view details of list of users associated with entered user group.

User Group – View



Field Description

Field Name	Description
Group Code	Display user group code

Field Name	Description
Group Description	Display description provided to the user group
User Information	
Username	Username of the user who is part of the user group is displayed. Click on the link to view the user details.
Name	Display name of the User.
Mobile Number	Display Mobile Number of the user that maintain with bank.

4. Click **Back** to navigate back to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.

15.5.3 User Groups – Edit

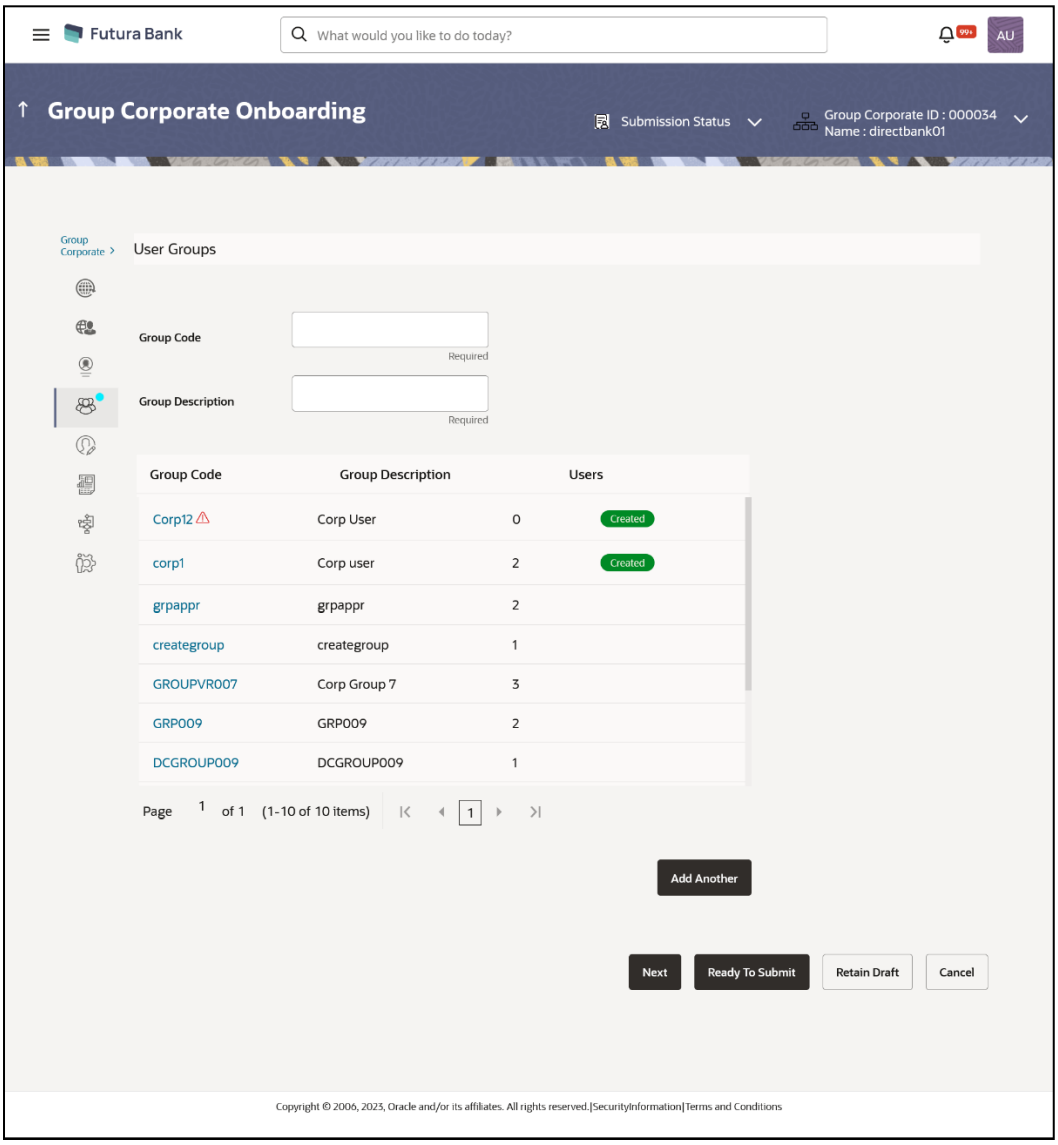
This function enables the Bank Administrator to edit the description of existing user groups mapped under Group Corporate. Bank Administrator can also add new users and remove existing users of the user group as part of this function.

A check is performed on minimum and maximum number of users allowed as a part of user group while adding or removing the users from the user group.

To edit or update a user group:

1. In **User Group Management** screen, in the **Group Code** or in **Group Description** enter the Respective details.
2. Click **Search**. User groups maintained if any under the Group Code or Group Description are displayed on the screen.

Summary screen

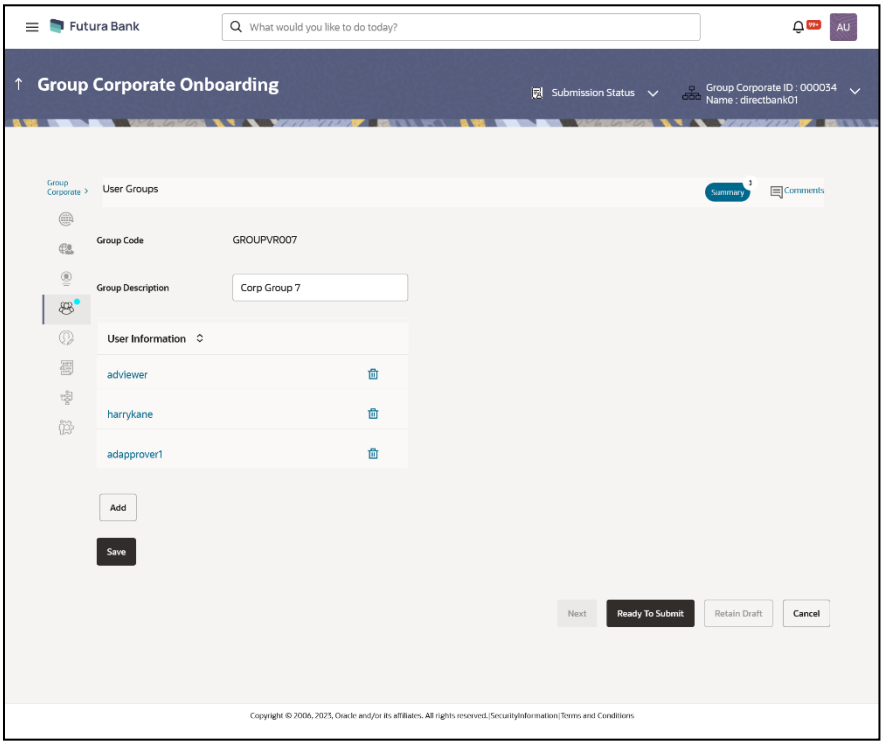


Field Name	Description
Search User Group	
Group Code	Enter User group code
Group Description	Enter Description provided to the user group.
Search Result	

Field Name	Description
Group Code	Display user group code
Group Description	Display description provided to the user group
User Count	Display Number of users available in each user group

3. Click on **Group Code** hyperlink to view details of list of users associated with entered user group.
4. Click **Edit** to edit the user group.
   The **User Groups - Edit** screen displays the mapping of the user group.
   OR
   Click **Cancel** to cancel the transaction.

User Group – Edit



Field Description

Field Name	Description
Edit	

Field Name	Description
Group Code	Display user group code
Group Description	Enter Description provided to the user group.
User Information	
Username	Username of the user who is part of the user group is displayed. Click on the link to view the user details.

5. In the User Group section, Click **Add** to add the selected user in the User Group. Once added, the user name will be removed from the user drop-down to avoid duplication of users.
   Click to remove a user from the User Group.
6. **Click Save** to save the maintenance, and redirect to the review page.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.
7. Click **Edit** to modify the details entered.
   OR
   Click on **Add Another** to add new User Group.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.

17. The success message of user group creation appears along with the transaction reference number.

15.6 Step 5: User Account Access

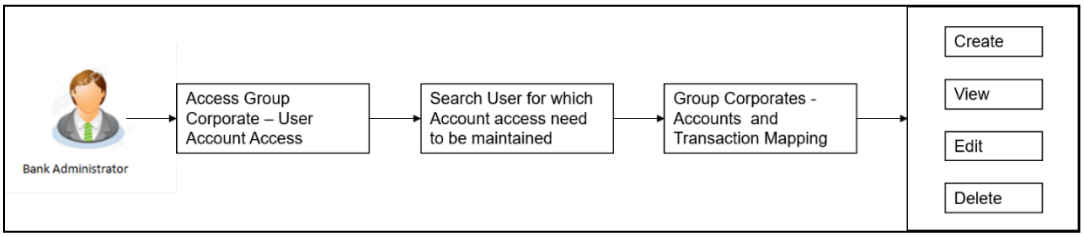
Using this option the Bank Administrator can set up account and transaction access for user(s) of the Group Corporate. This maintenance can be done only after the Party Account Access is setup for the parent party of the user(s). The user level mapping of accounts and transactions must be done to provide access to the accounts for performing transactions to the specific user. If this step is not followed, the corresponding user will not be able to view any accounts on the dashboard screen or at the individual transactions.

Note: User Account Access is a non-mandatory step. If the Admin does not maintain the user account access for any of the corporate users, system will refer to the party account access rules maintained for his associated party ID.

Pre-Requisites

- Account Access should be maintained for the corporate party of the user for which access is to be maintained
- Account Access for the party should be maintained for associated party accounts if the user needs access to associated party accounts.
- Party preferences should be created for the party of the user for which access is to be maintained
- Channel Access should be enabled for party of the user for which account access is to be maintained
- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.

Workflow



Features Supported In Application

The following options are available as part of this maintenance:

- User Account Access - Mapping
- User Account Access – View
- User Account Access - Edit
- User Account Access - Delete

How to reach here:

System/ Bank Administrator Dashboard > Corporate Onboarding > Group Corporate Onboarding > User Account Access

OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Group Corporate Onboarding > User Account Access

15.6.1 User Account Access – Create

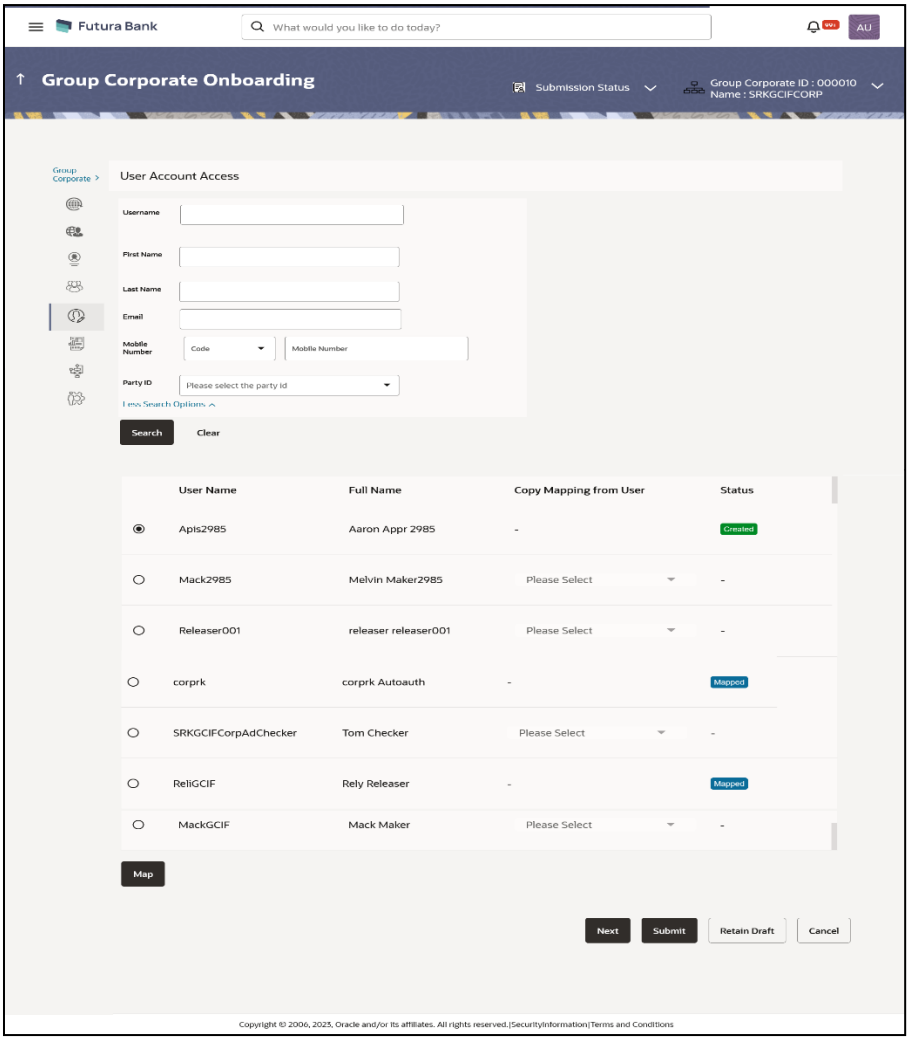
Using this option, Bank Administrator can maintain Accounts and Transaction access for the corporate users associated with a specific Group Corporate ID.

This option lets the administrator to provide account access to specific users of a party.

To provide the user with account and transaction access:

1. In the **User Search** field search users for whom Transaction Account access need to be maintained.
   OR
   Select the user from list displayed below.
2. Select the user ID and click on "**Map**" to navigate to **Account Access summary**

User Account Access – Search and Search Result



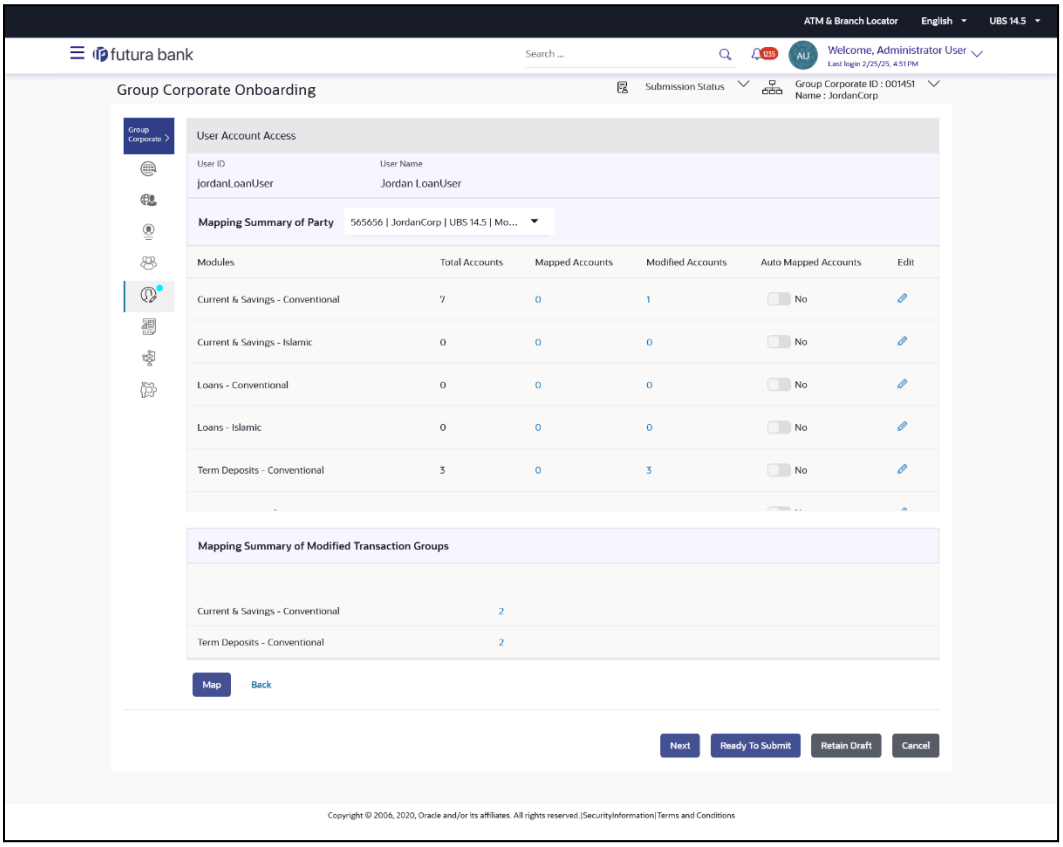
Field Description

Field Name	Description
User Name	To search the user with the user name. Partial search is allowed.
More Search Options	
Below fields appears if you click the **More Search Options** link.	
First Name	Allows to search based on first name or given name of the user.
Last Name	Allows to search based on last name/ surname of the user.
Email	Allows to search based on email id of the user.
Mobile Number	Allows to search based on mobile number of the user. Note: Select international subscriber dialing (ISD) code along with the mobile number to search the user.
Party ID	Allows to search based on Party id.
Search Result	
User ID	User ID the corporate user
User Name	User name of the corporate user
Copy Mapping from User	Select this to Inherit and copy account maintenance from already setup user to new user
Status	Displays the account mapping status for the corporate user. • **Mapped**: Corporate user for which accounts mapping is being done and authorized. • **Modified**: Corporate user for which accounts mapping is being done but pending approval by authorizer. • **Deleted:** Corporate user for which accounts mapping is deleted.

3. From the **Mapping Summary of Party** dropdown list, select the corporate party id associated with Corporate User.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

4. For a searched user, summary screen will be displayed with total accounts associated with corporate party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .

User Account Access – Summary



Field Description

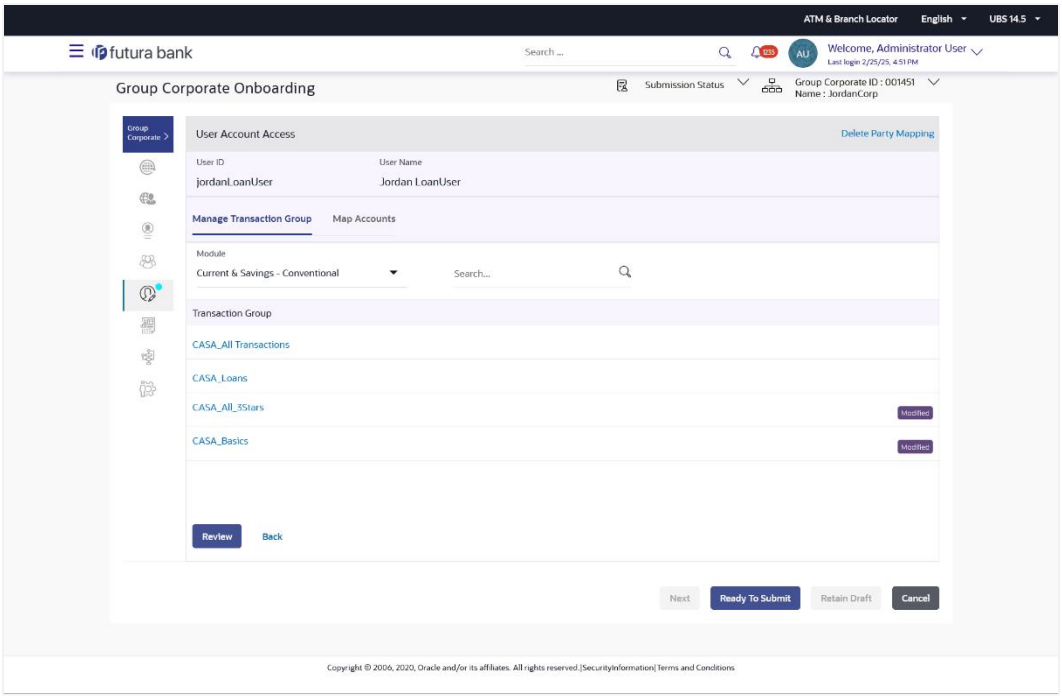
Field Name	Description
User ID	User ID the corporate user
User Name	User name of the corporate user
Mapping Summary of Party	The corporate party for which Party accounts access is being viewed
Modules	Banking module names.
Total Accounts	Total number of accounts available under the party that can be map with corporate user.

Field Name	Description
Mapped Accounts	Number of accounts mapped to the particular account type of corporate user.
Modified Accounts	Number of accounts modified for the particular account type of corporate user.
Auto Mapped Accounts	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided
Mapping Summary of Modified Transaction Group	
Modules	Banking module names.
Modified Groups	Number of transaction groups modified for the particular module.
Edit or Map	Click on the icon next to every module or click on Map button to edit User account access

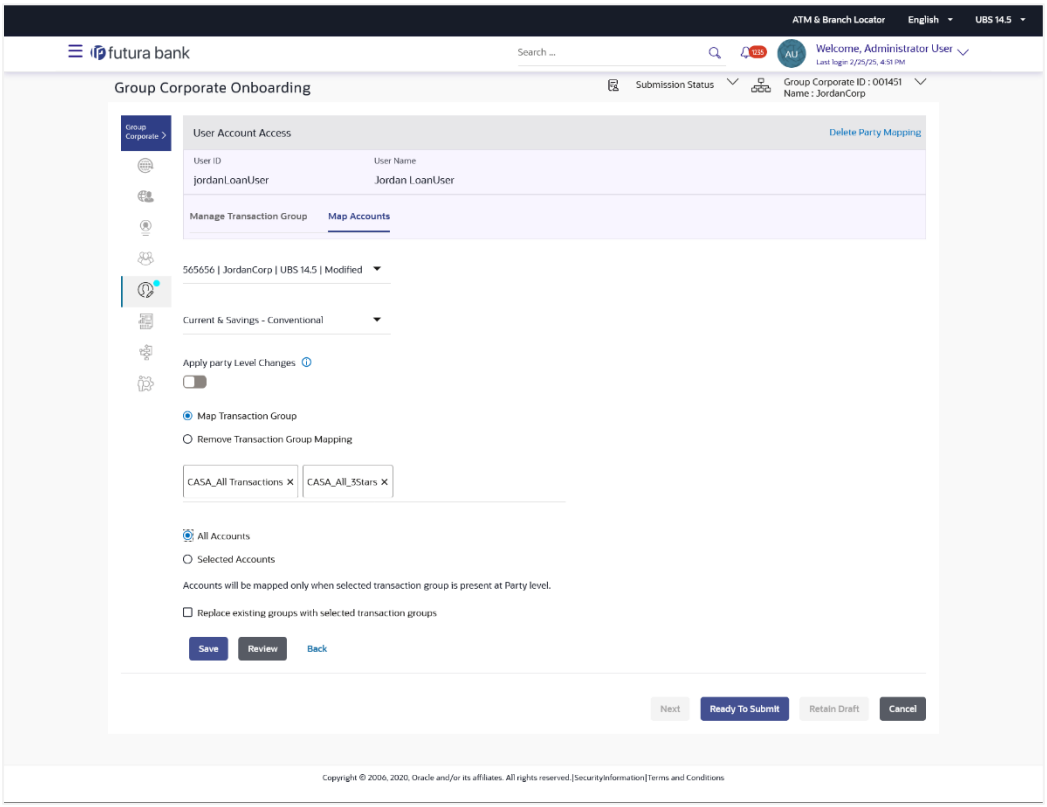
5. If there is no mapping done for a user, the count for the **Mapped Accounts** will be '**0'.**
6. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories i.e. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts along with Liquidity Management enabled Real Accounts (including External Accounts if any) and VAM enabled Real and virtual accounts for a Corporate.
7. User Account Access will inherit the account access setup at the party level for all the parties associated to him (party association will be done at the time of user onboarding in user management screen). The screen will show the inherited Maintenance in User Account Access screen. In the **Auto Mapped Accounts** field, toggled **ON** to allow access to all future Accounts across banking module.
   OR
   In the **Auto Mapped Accounts** field, toggled **OFF** to explicitly map new accounts and transactions manually.
8. Click on the **Modified Groups** count link to view the details of transaction groups details.
7. Click **Map** or **Edit** (available across each banking module). The **User Account Access - Create** screen appears.
   OR

Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate to the previous screen.

User Account Access – Manage Transaction Group Tab



User Account Access – Map Accounts Tab



Field Description:

Field Name	Description
User ID	User ID the corporate user for whom account access in being setup
User Name	User name of the corporate user
Manage Transaction Group Tab	
Module	Select Banking Module types available under the selected party to setup account access.

Field Name	Description
Select Transaction Groups	Select the Transaction group to map transactions and maintain access in Account Access screens. Note : 1) Transaction groups mapped to the accounts at party level will be shown on this screen. 2) In user account access, the accounts can be mapped to the same transaction group to which the accounts are mapped at the party level
Transactions Groups	Search and add the transaction groups.
Map Accounts Tab	
Mapping Summary of Party	The corporate party for which user accounts access is being viewed.
Modules	Select Banking Module available under the selected party to setup account access
Apply Party level Changes	Toggle to enable to apply party level changes automatically.
Action	Option to map/unmap the transactions and maintain access in Account Access screens of Transaction Groups. The options are: • Map Transaction Group • Remove Transaction Group Mapping **Note**: Only one transaction group can be unmapped at a time. A transaction group can be unmapped from All Accounts or Selected Accounts.

Field Name	Description
Account Selection	Select accounts to map the transaction groups. The options are: • All Accounts - map selected transaction groups to all accounts within the system. • Selected Accounts - map transaction groups to selected accounts **Note:** **1)** System will show a tag as 'Modified' followed by the transaction group name after the account number. 2) Accounts will be mapped only when selected transaction group is present at Party Level.
All Accounts	Click to select all the accounts available under the selected module.
Selected Accounts	Search and select the account(s) using using various search criteria.
Filter Criteria	
Account Number	Search by entering a complete or partial account number (minimum of 5 characters).
Transaction Groups	Search for accounts currently mapped with specific transaction groups.
Account Access Status	Search for accounts based on their account access status.
Account Status	Search for accounts based on their current status.
Account Currency	Search for accounts based on account currency.
Search Result	

Field Name	Description
Account Numbers	Displays the list of accounts based on search criteria. Note: Administrator can select one or multiple accounts from the result. Information presented with each listed account number includes the Account Name, Account Currency, Transaction Group, and Branch Code.
Number of Accounts Selected	Number of accounts selected under the particular module.
Replace existing groups with selected transaction groups	Select this option to replace the existing transaction group mappings with the newly selected transaction groups. Note: If the option is not checked, the selected transaction groups are appended to the already mapped groups for the account.
Delete Party Mapping	Click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate users in one step.

12. In the **Map Accounts** Tab;
    i. From the **Module** list, select the factory shipped **Transaction group** under selected module which will have all transactions and inquiries grouped together.

Note: Factory shipped user group cannot be deleted or modified.

    ii. In the **Apply Party Level Changes** field, toggle to enable to apply party level changes automatically.
    iii. In **Action** field, select the desired option to map/ unmap the Transaction Group.
    iv. If the **Map Transaction Group** option is selected;
        1. In the **Transaction Group**s list, select the transaction Group/s to map / unmap from the drop-down list.
        2. In **Account Selection** field, select the option to map the transaction groups to all the accounts or specific accounts.
        3. Map single or multiple transaction groups to either all accounts or specific selected accounts.
            i. If All Accounts option is selected, the transaction groups will be mapped to all available accounts.

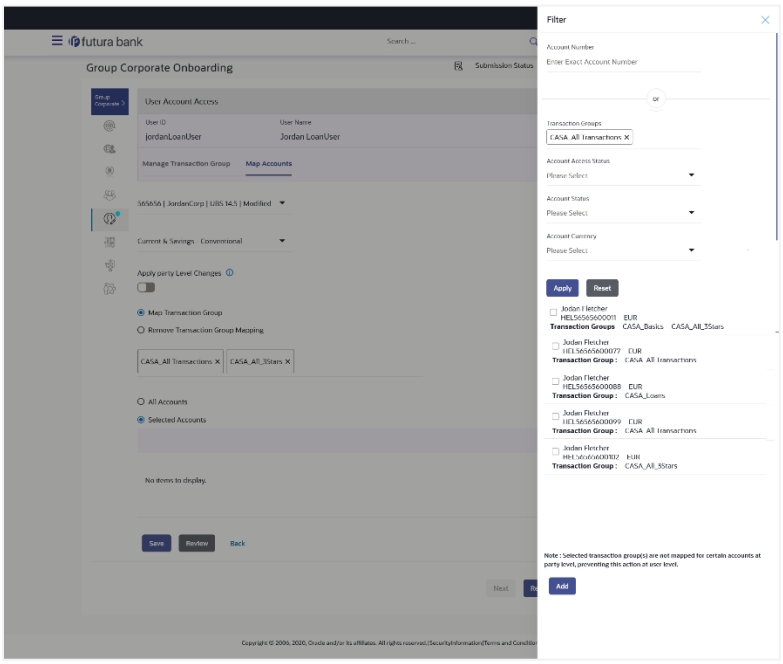
ii. If the **Selected Accounts** option is selected ,
Click the icon. The **Filter** overlay screen appears where administrators can search for accounts using various criteria like Account Number, Accounts with Mapped Transaction Groups, Account Status, Account Currency.
a. Click **Apply** to search the accounts based on the search criteria. The list of accounts gets displayed based on criteria entered.
b. Select the one or multiple accounts from the results by selecting the respective check boxes preceding the account number.
c. Click **Add**. The account(s) gets added for mapping to transaction groups.

Note:
1) Click **Add More Accounts** to add additional accounts for mapping to transaction group
2) Additional Mapping Considerations

If a specific transaction group mapping is unavailable for an account at the party level, the account number will be displayed in a disabled form and will not be available for selection.

Administrators have the option to add additional accounts from the accounts selected in a previous set.

Map Transaction Group – Filter Criteria



OR
Click **Reset** the clear the details entered.

4. Select the **Replace existing groups with selected transaction groups** field, user can **unmap** the accounts by selecting accounts and then clicking on **Unmap** to reset their mapping with Group Corporate.
   a. Choose the desired option;
   If the checkbox is checked, the system will replace existing transaction group mappings with the newly selected groups; otherwise, the selected groups are added to the existing mappings.

13. Upon user account mapping, the system appends a **Modified** tag followed by the transaction group name to the account number.
14. To map the new accounts, select appropriate option from **Auto Map** toggle button;
    Select **Auto** if you wish to allow access to all future Accounts across banking module.
    OR
    Select **Manual** if you wish to explicitly map new accounts and transactions.
15. User can click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate user in one step.
16. Click **Save** to map the transaction groups to the selected accounts.
    OR
    Click **Review** screen appears. Verify the details, and click **Submit.**
    OR
    Click **Back** to navigate back to previous screen.

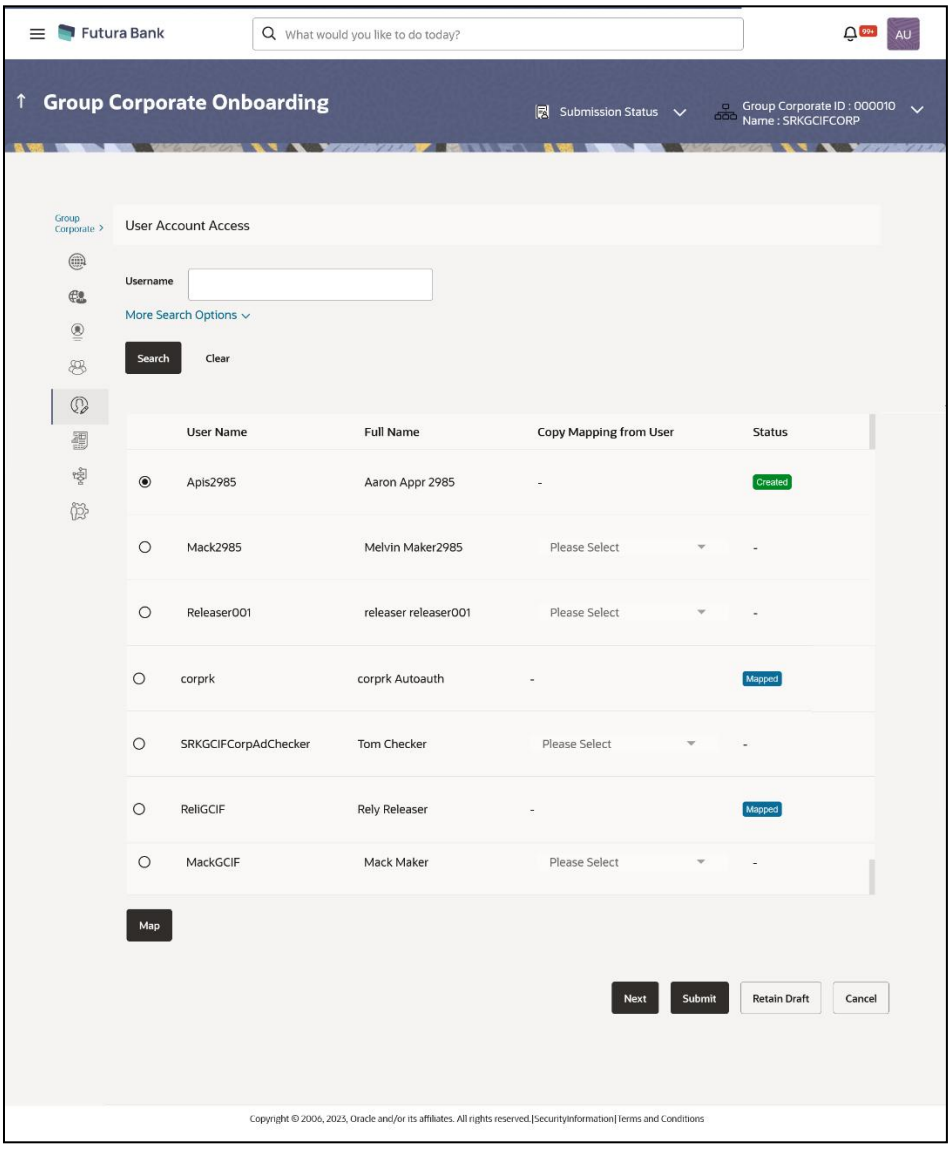
15.6.2 User Account Access – View

The Bank Administrator can view the list of account(s) and transactions for which access has been provided to the user.

To view the account and transaction access:

1. In the **User Search** field search users for whom Transaction Account access is being viewed.
   OR
   Select the user from list displayed below.
2. Select the user ID and click on “Map” to navigate to **Account Access summary**.

User Account Access – Search and Search Result

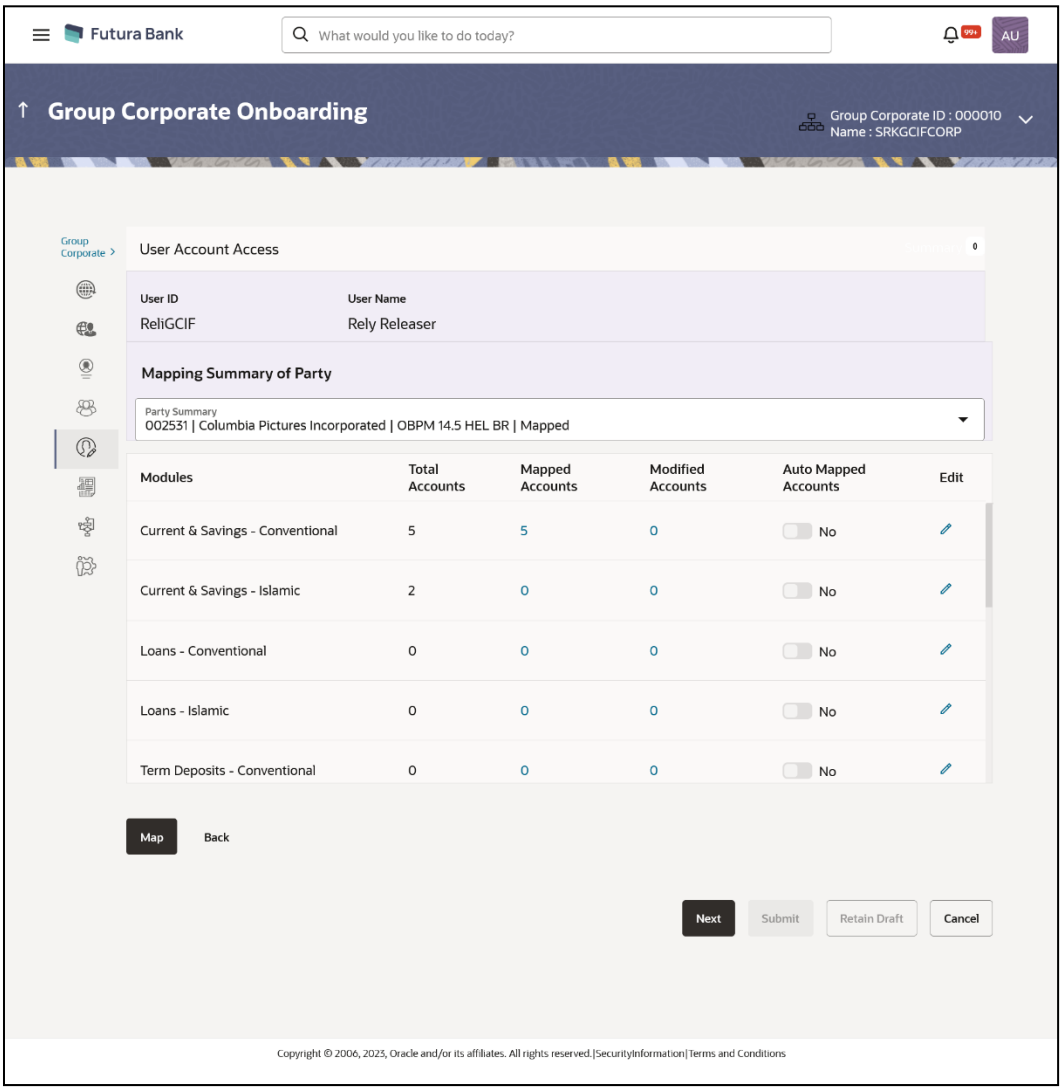


Field Description

Field Name	Description
Search (User)	User quick search panel so search user for setting up the account access.
Search Result	
User ID	User ID the corporate user
User Name	User name of the corporate user
Copy Mapping from User	Select this to Inherit and copy account maintenance from already setup user to new user
Status	Displays the account mapping status for the corporate user. • **Mapped**: Corporate user for which accounts mapping is being done and authorized. • **Modified**: Corporate user for which accounts mapping is being done but pending approval by authorizer. • **Deleted:** Corporate user for which accounts mapping is deleted.

3. From the **Mapping Summary of Party** dropdown list, select the corporate party id associated with Corporate User.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
4. For a searched user, summary screen will be displayed with total accounts associated with corporate party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .

User Account Access - Summary Results



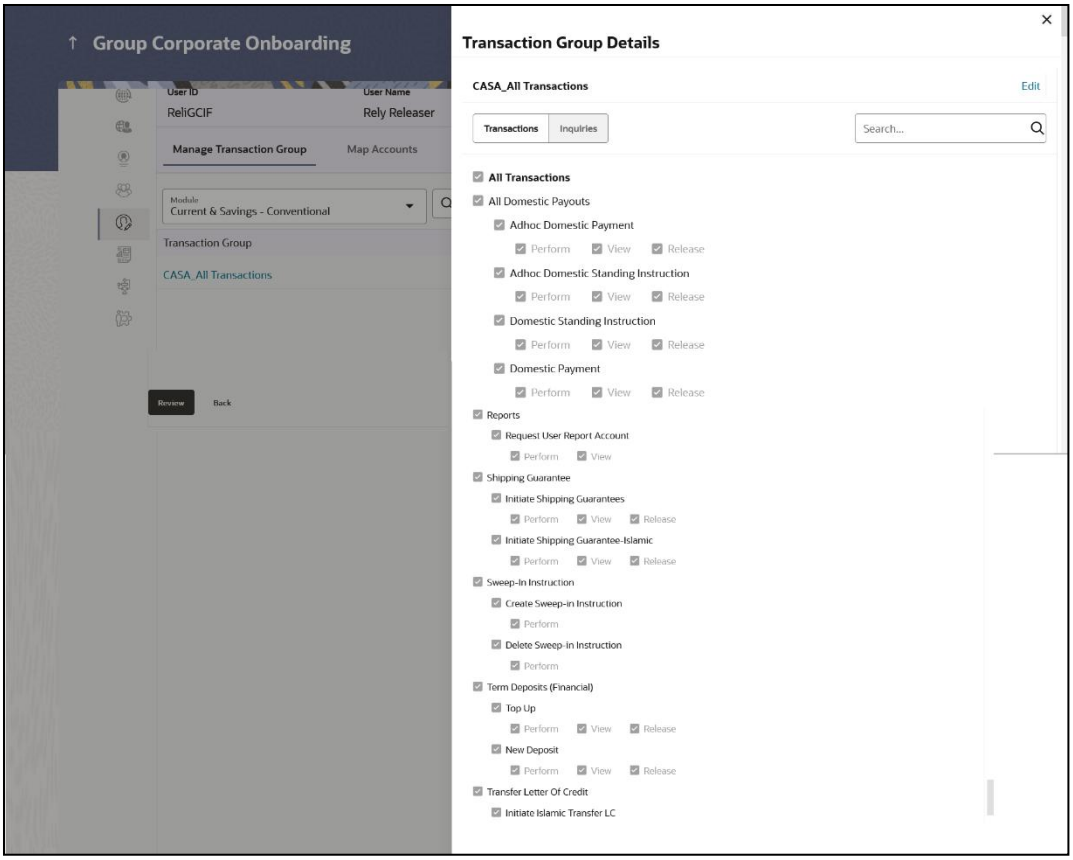
Field Description

Field Name	Description
User ID	User ID the corporate user
User Name	User name of the corporate user
Mapping Summary of Party	The corporate party for which Party accounts access is being viewed
Modules	Banking Module names

Field Name	Description
Total Accounts	Total number of accounts available under the party that can be map with corporate user.
Mapped Accounts	Number of accounts mapped to the particular account type of corporate user.
Modified Accounts	Number of accounts modified for the particular account type of corporate user.
Auto Mapped Accounts	Mapping status of the accounts. The options can be: • **Auto**: gives default access to all newly added accounts and transactions of the party as soon as the account is opened in future. • **Manual**: gives specific access to future accounts. The new accounts and transactions need to be mapped explicitly if access needs to be provided
Edit or Map	Click on the icon next to every module or click on Map button to edit User account access

5. If there is no mapping done for a party, the count for the **Mapped Accounts** will be '**0'**
6. All the accounts held by the selected party as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories

User Account Access – View



Field Description:

Field Name	Description
Modules	Display name of the product for which account access is being viewed.
Mapped Transaction Group	Display the transaction groups selected to setup the user account access.
Transaction Groups Details	Display the Transaction group details with which user account access is maintained along with transaction and inquiries mapped to it.

7. The User Account Access details screen has two section. First section displays the lists down all the transaction groups mapped.
8. In the second column, user can view the **transaction group** details with all the transactions and inquiries access.
9. Click **Edit / Map** to update the **User Account Access** account mapping for new accounts and existing accounts.
   OR

Click **Back** to navigate to the previous screen.
OR
Click **Next** to proceed to the next logical step.
OR
Click **Submit** to submit the steps performed so far for approval.
OR
Click **Retain Draft** to save the details entered as draft.
OR
Click **Cancel** to cancel the transaction.

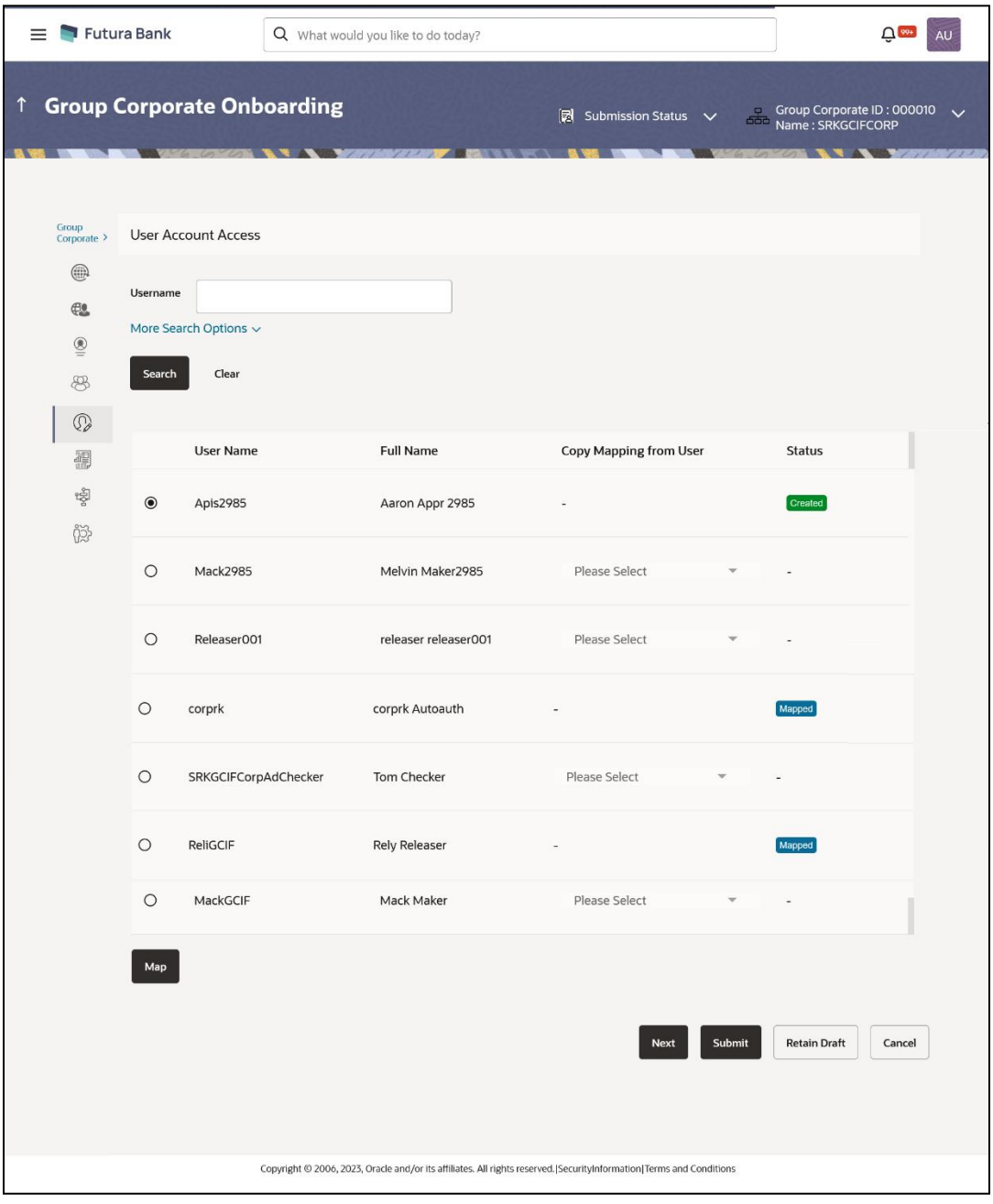
15.6.3 User Account Access – Edit

The Bank Administrator gets a request with the list of account(s) and transactions for which access details needs to be edited for a selected user of the party.

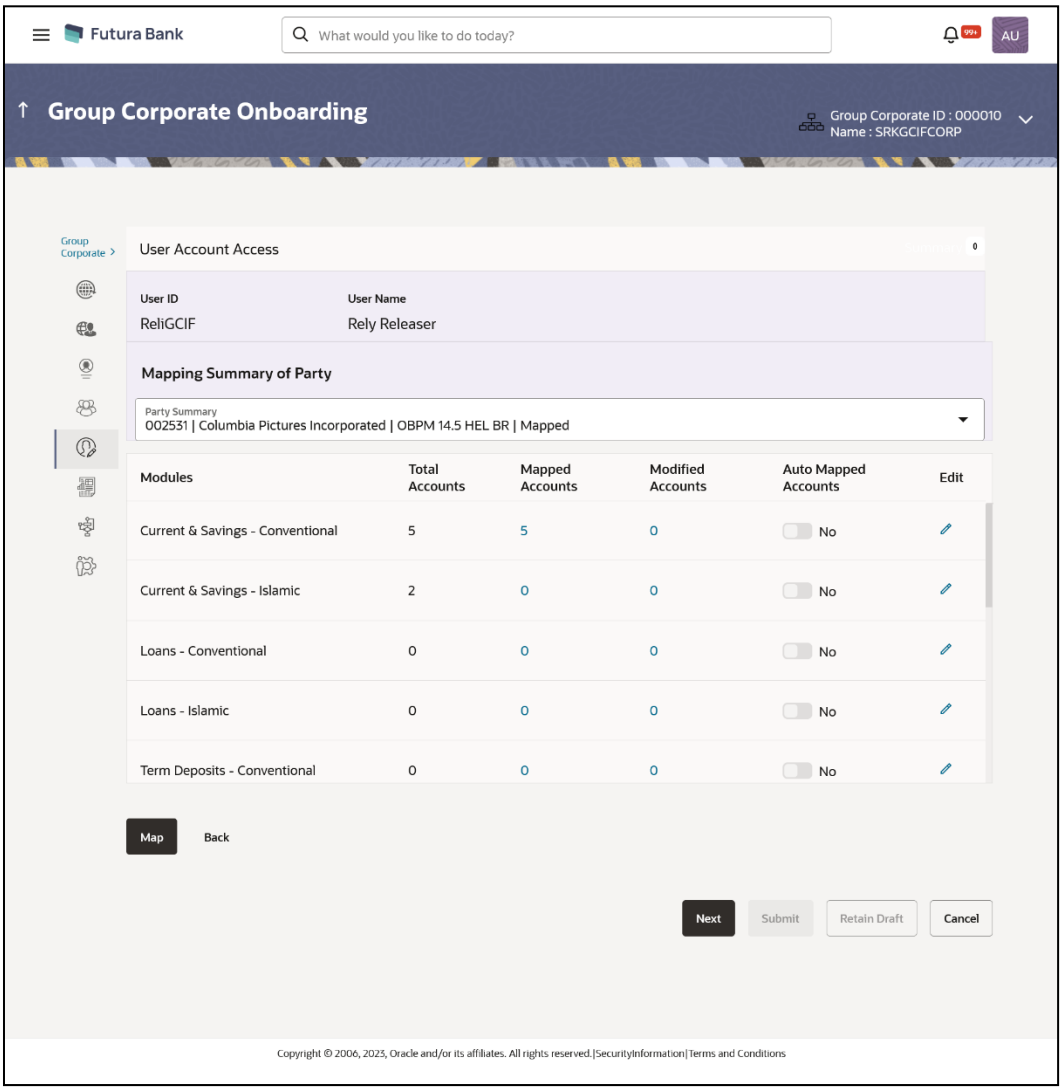
To Search and Edit the User account and transaction access:

1. In the **User Search** field search users for whom Transaction Account access is to modify.
   OR
   Select the user from list displayed below.
2. Select the user ID and click on “Map” to navigate to **Account Access summary**
3. From the **Mapping Summary of Party** dropdown list, select the corporate party id.
4. For a searched user, summary screen will be displayed with total accounts associated with corporate party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .
5. Click the link under the total **Mapped accounts** or **Modified accounts**, The **User Account Access – View** (Transaction Mapping) screen appears. . The search result according to the search criteria appears
   OR
   Click **Cancel** to cancel the transaction.
6. If there is no mapping done for a user, the count for the **Mapped Accounts** will be ‘**0’.**
7. All the accounts held by the selected user as a relationship with the bank as available in the core banking system or the respective mid-office system will be fetched and displayed in the respective categories
8. Click **Map** or **Edit** (available across each banking module). The **User Account Access - Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.

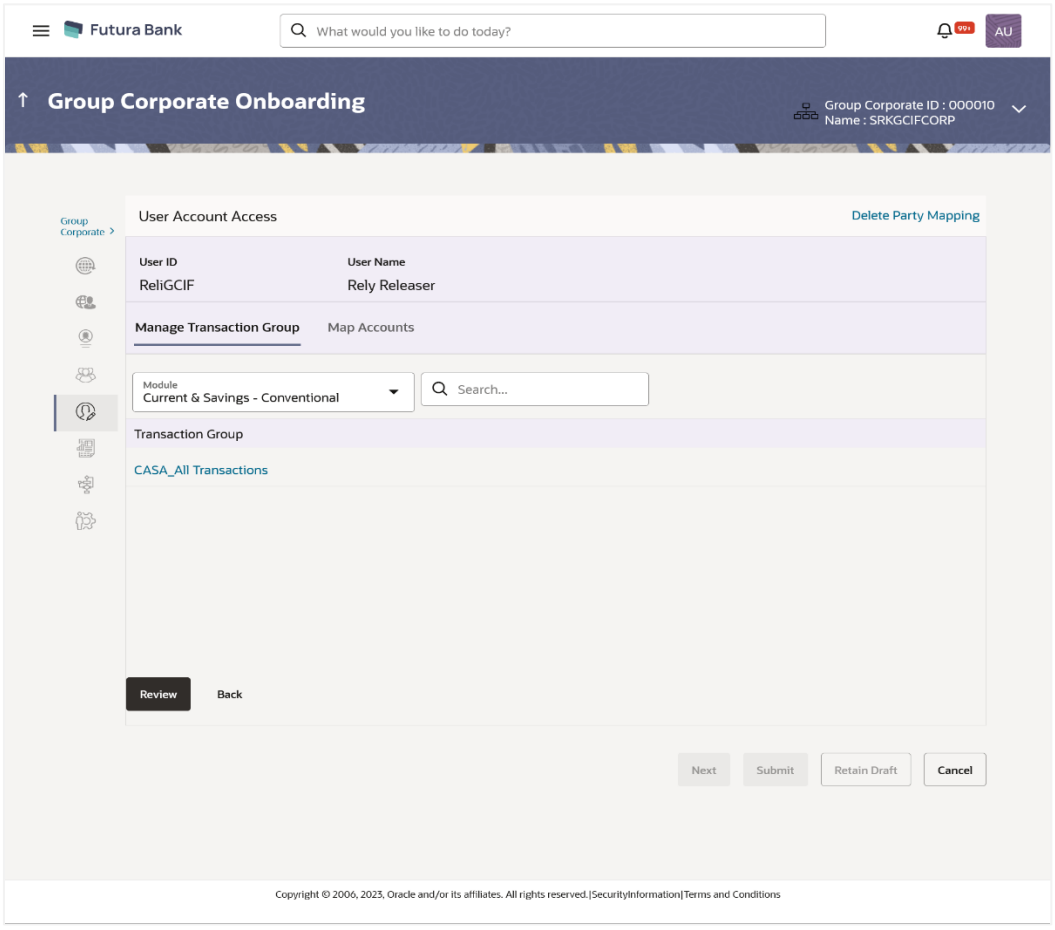
User Account Access – Search and Search Result



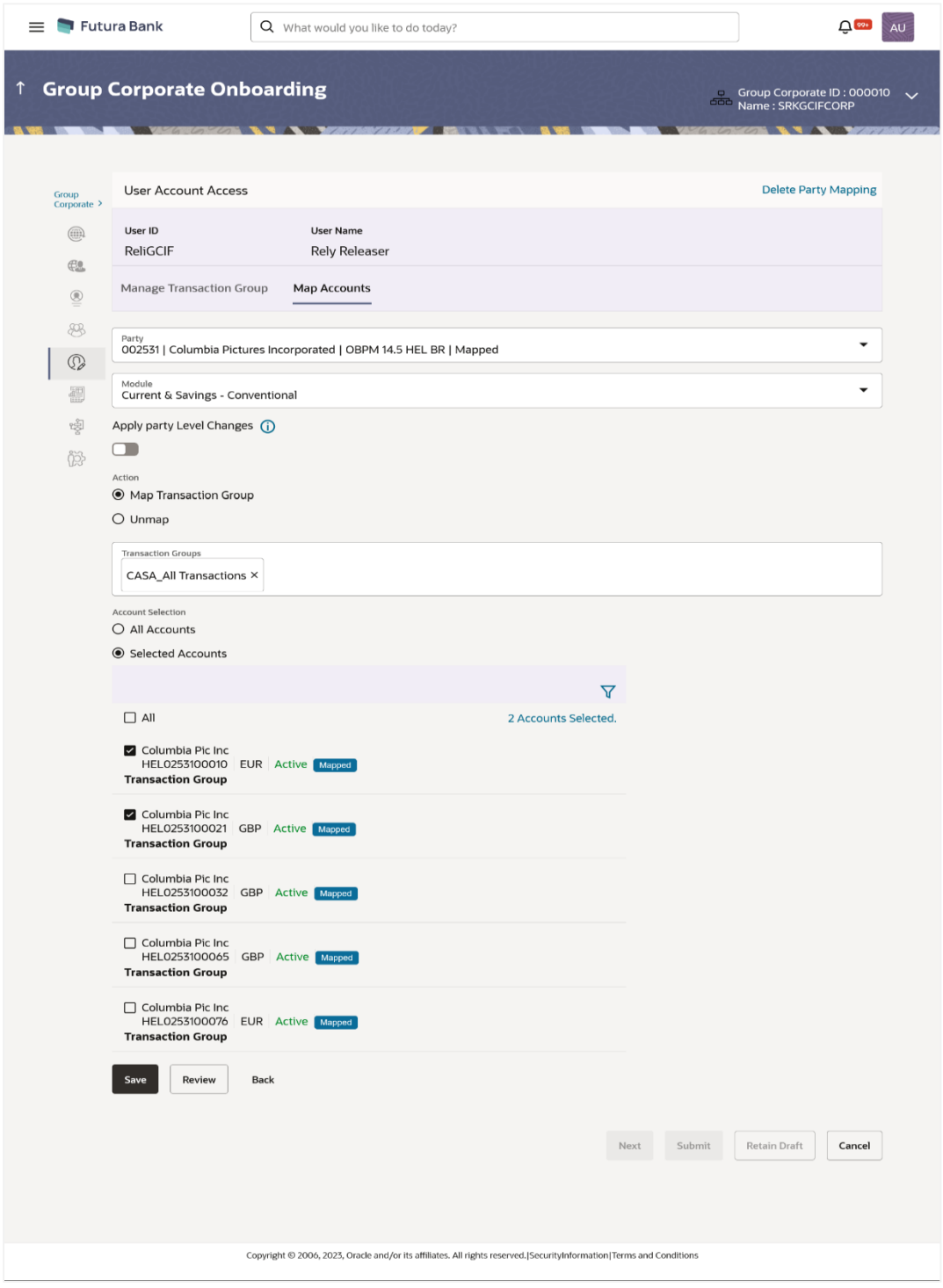
User Account Access – Summary



User Account Access – Manage Transaction Group



User Account Access – Map Accounts Tab



9. The User Account Access screen has four section. Header of the screen shows the User ID and User Name. First column lists down all the **modules** in tabular form, second column list

down the **transaction groups** and third column list down banking module wise **account number**

10. Navigate and select specific **module** tab (Including viz. Current and Savings Accounts for both Conventional and Islamic, Credit Card, Term Deposit, Loan accounts along with Liquidity Management enabled Real Accounts (including External Accounts if any) and VAM enabled Real and virtual accounts for a Corporate.) in the first column for which account and transaction access mapping maintenance need to be setup.
11. In the second column, There will be one factory shipped **Transaction group** for each module, which will have all transactions and inquiries grouped together.

Note: Factory shipped user group cannot be deleted or modified.

12. Once the transaction groups are created, user can select specific module , along with the transaction groups and can select 'All Accounts' to map the selected transaction group/s to all the existing accounts under the selected party
    OR
    If transaction groups need to be mapped to specific accounts, then the user needs to select the respective check boxes preceding the account number.
13. Once the user maps the accounts, system will show a tag as **'Modified'** followed by the transaction group name after the account number.
14. To map the new accounts, select appropriate option from **Auto Map** toggle button;
    Select **Auto** if you wish to allow access to all future Accounts across banking module.
    OR
    Select **Manual** if you wish to explicitly map new accounts and transactions.
15. User can **unmap** the transaction groups by selecting accounts and then clicking on Save button to reset their mapping with Group Corporate
16. User can click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate user in one step.
17. User can drill down his search by applying Filter to search an account basis on Transaction Group, currency, mapping status
18. Click **Save** to save the maintenance, and redirect to the review page.
    OR
    Click **Next** to proceed to the next logical step.
    OR
    Click **Submit** to submit the steps performed so far for approval.
    OR
    Click **Retain Draft** to save the details entered as draft.
    OR
    Click **Cancel** to cancel the transaction.

Note: Admin can submit the maintenance after any step. Maintenances saved so far will be sent for approval in one flow. Admin would not be able to make any changes or maintain another step for the same Group Corporate till the time the approval of the wizard is not done.

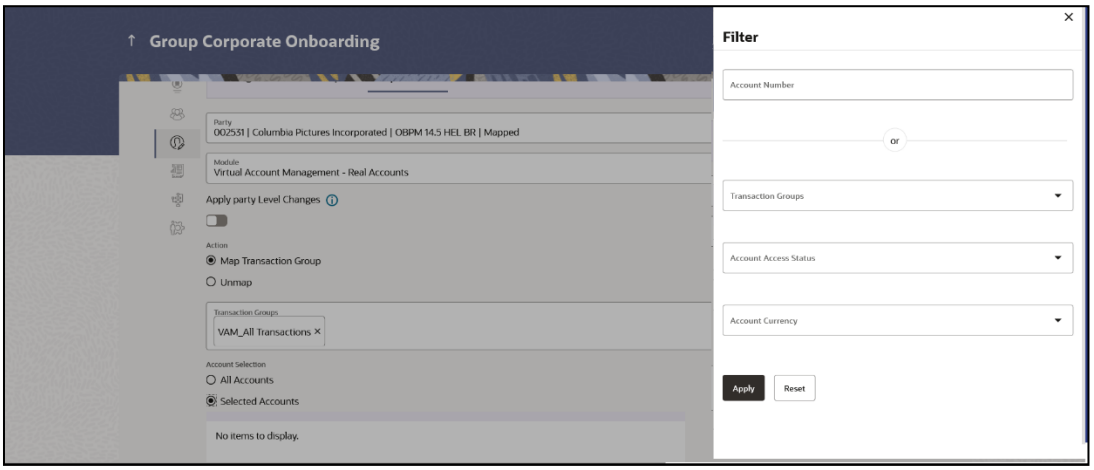
19. The **Review** screen appears. Verify the details, and click **Submit**.
    OR
    Click **Edit** to modify the details entered.
    OR
    Click **Next** to proceed to next step.
    OR

Click **Retain Draft** to save all the steps completed so far, and allow Admin resume the same application.
OR
Click **Cancel** to cancel the transaction.

20. The success message of user creation appears along with the transaction reference number

Note : Following flow explains the Drill down options to search by applying Filter to search an account for Virtual Accounts Management & Liquidity Management module.

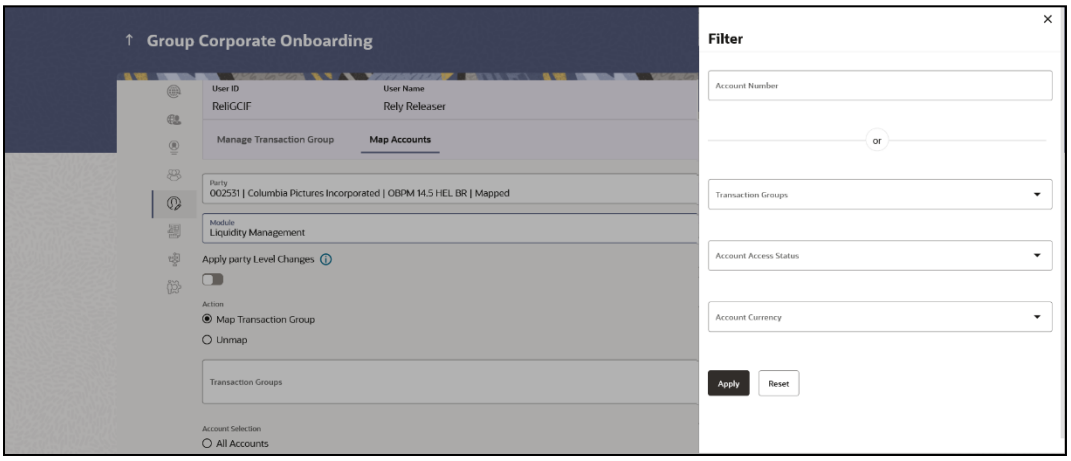
Virtual Account Management (Real Account) Tab



To view Virtual Account Management - Real Accounts:

1. In the **Account Number** field, enter the exact Real Account number.
   OR
   From the **Branch name** drop down, select the Branch name.
   OR
   From the **Account Access Status** field, select an appropriate status.
   OR
   From the **Currency** field, select the required currency.
2. Click **Apply** to Apply the filter.
   OR
   Click **Reset** to reset the entered data.
3. The user can filter through two sections :
   1. On the basis of the Account Number
      OR
   2. A combination of branch name, currency filters and other parameters. The user can use these search parameters alone or in a combination to filter search results.

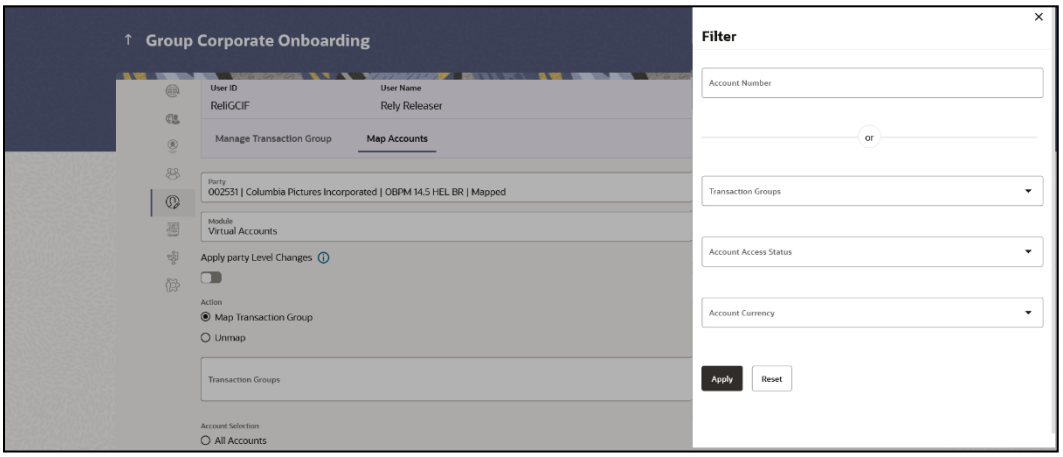
Liquidity Management Tab



To view Liquidity Management Accounts:

1. In the **Account Number** field, enter the exact Real Account number.
   OR
   From the **Branch name** drop down, select the Branch name.
   OR
   From the **Account Access Status** field, select an appropriate status.
   OR
   From the **Currency** field, select the required currency.
2. Click **Apply** to Apply the filter.
   OR
   Click **Reset** to reset the entered data.
3. The user can filter through two sections :
   1. On the basis of the Account Number
      OR
   2. A combination of branch name, currency filters and other parameters. The user can use these search parameters alone or in a combination to filter search results.

Virtual Accounts Tab



To view Virtual Accounts:

1. In the **Virtual Account Number** field, enter the exact Virtual Account number.
   OR
   In the **Virtual Account Name** field, enter the Virtual account name.
   OR
   From the **Virtual Entity** search, select the Virtual Entity name.
   OR
   From the **Branch name** drop down, select the Branch name.
   OR
   From the **Account Access Status** field, select an appropriate status.
   OR
   From the **Status** drop down, select the status.
   OR
   From the **Currency** field, select the required currency.
2. Click **Apply** to apply the filter.
   OR
   Click **Reset** to reset the entered data.
3. The user can filter through two sections :
   1. On the basis of the Account Number
      OR
   2. A combination of branch name, currency filters and other parameters. The user can use these search parameters alone or in a combination to filter search results.

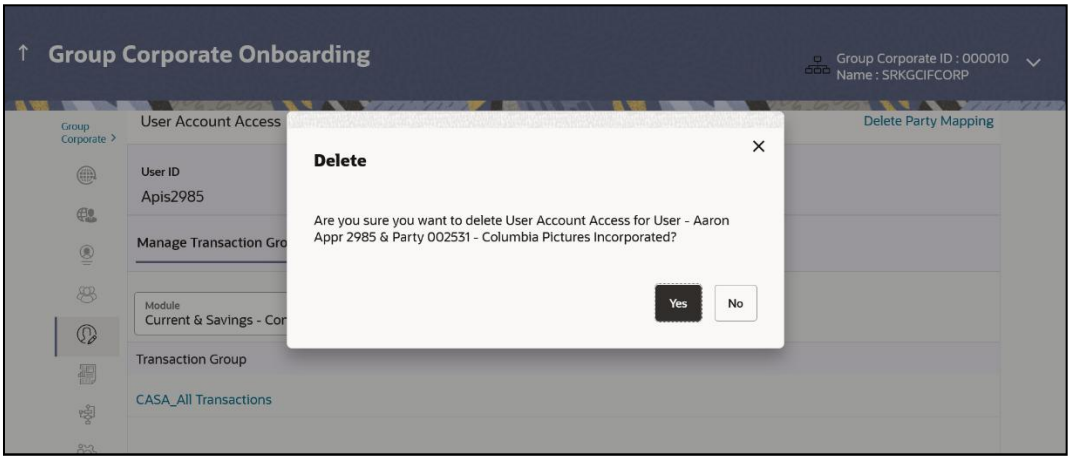
15.6.4 User Account Access – Delete

The Bank Administrator gets a request with the user information of a party for which access details needs to be deleted. As part of this option, account mapping can be deleted for a user.

To delete account and transaction access for the User:

1. In the **User Search** field search users for whom Transaction Account access is to modify.
   OR
   Select the user from list displayed below.
2. Select the user ID and click on “Map” to navigate to **Account Access summary.**
3. From the **Mapping Summary of Party** dropdown list, select the corporate party id.
4. For a searched user, summary screen will be displayed with total accounts associated with corporate party of that user, status of the accounts mapped for the internet banking for user, modified accounts if any and Auto account mapping status .
5. Click the link under the total **Mapped accounts** or **Modified accounts**, The **User Account Access – View** (Transaction Mapping) screen appears. . The search result according to the search criteria appears.
   OR
   Click **Cancel** to cancel the transaction.
6. User can click on **Delete Party Mapping** to delete all the Transaction and account access maintenance done for corporate user in one step.

User Account Access – Delete party Mapping



   a. Click **Yes** to delete the party mapping.
      OR
      Click **No** to cancel the process.
7. Click **Save** to save the maintenance, and redirect to the review page.
   OR

Click **Next** to proceed to the next logical step.
OR
Click **Submit** to submit the steps performed so far for approval.
OR
Click **Retain Draft** to save the details entered as draft.
OR
Click **Cancel** to cancel the transaction.

Note: Admin can submit the maintenance after any step. Maintenances saved so far will be sent for approval in one flow. Admin would not be able to make any changes or maintain another step for the same Group Corporate till the time the approval of the wizard is not done.

8. **The Review** screen appears. Verify the details, and click **Submit**.
   OR
   Click **Edit** to modify the details entered.
   OR
   Click **Next** to proceed to next step.
   OR
   Click **Retain Draft** to save all the steps completed so far, and allow Admin resume the same application.
   OR
   Click **Cancel** to cancel the transaction.
9. The success message of user creation appears along with the transaction reference number

15.7 Step 6: Report Mapping

The user report mapping maintenance allows the Bank Administrators to map the report or set of reports to first to at group corporate level and then at the a specific corporate user. The corporate users can generate and view the reports to which they have an access. If 'map to all user' option is enabled , then the reports mapped at the group corporate level will be automatically mapped to all the user in the group Corporate. If disabled, you can select the user and map the reports manually.

Bank Administrator searches a corporate user, onboarded on Group corporate and view the reports mapped to him, he can also un-map the reports from specific corporate user so that access of the specific report/ s can be removed to that corporate user.

How to reach here:

System/ Bank Administrator Dashboard > Corporate Onboarding > Group Corporate Onboarding > Report Mapping tab
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Group Corporate Onboarding > Report Mapping tab

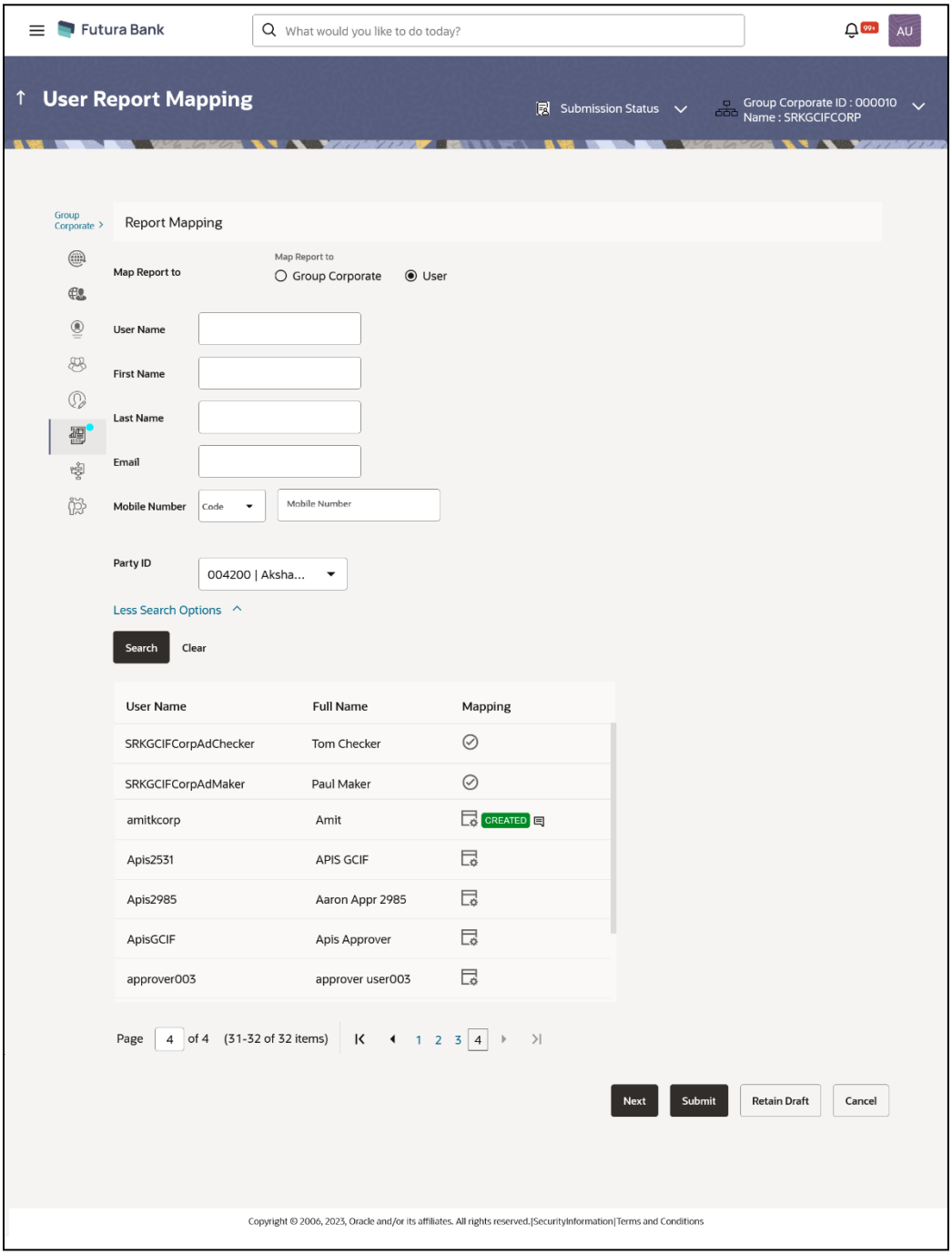
15.7.1 User Report Mapping – Search & View

Using this option Bank Administrator can search and view the reports mapped to the user.

To search and view the reports mapping:

1. In the **Map Report to** field, select the appropriate option whose mapped reports to be viewed.
    a. If you select **Group Corporate** option;
        i. System displays the report mapping summary at group corporate level.
    b. If you select **User** option;
        i. Enter the search criteria, click **Search**. The **User Report Mapping** screen with search results appears.
        OR
        Click **Clear** to clear the search parameters.
        OR
        Click **Cancel** to cancel the transaction.

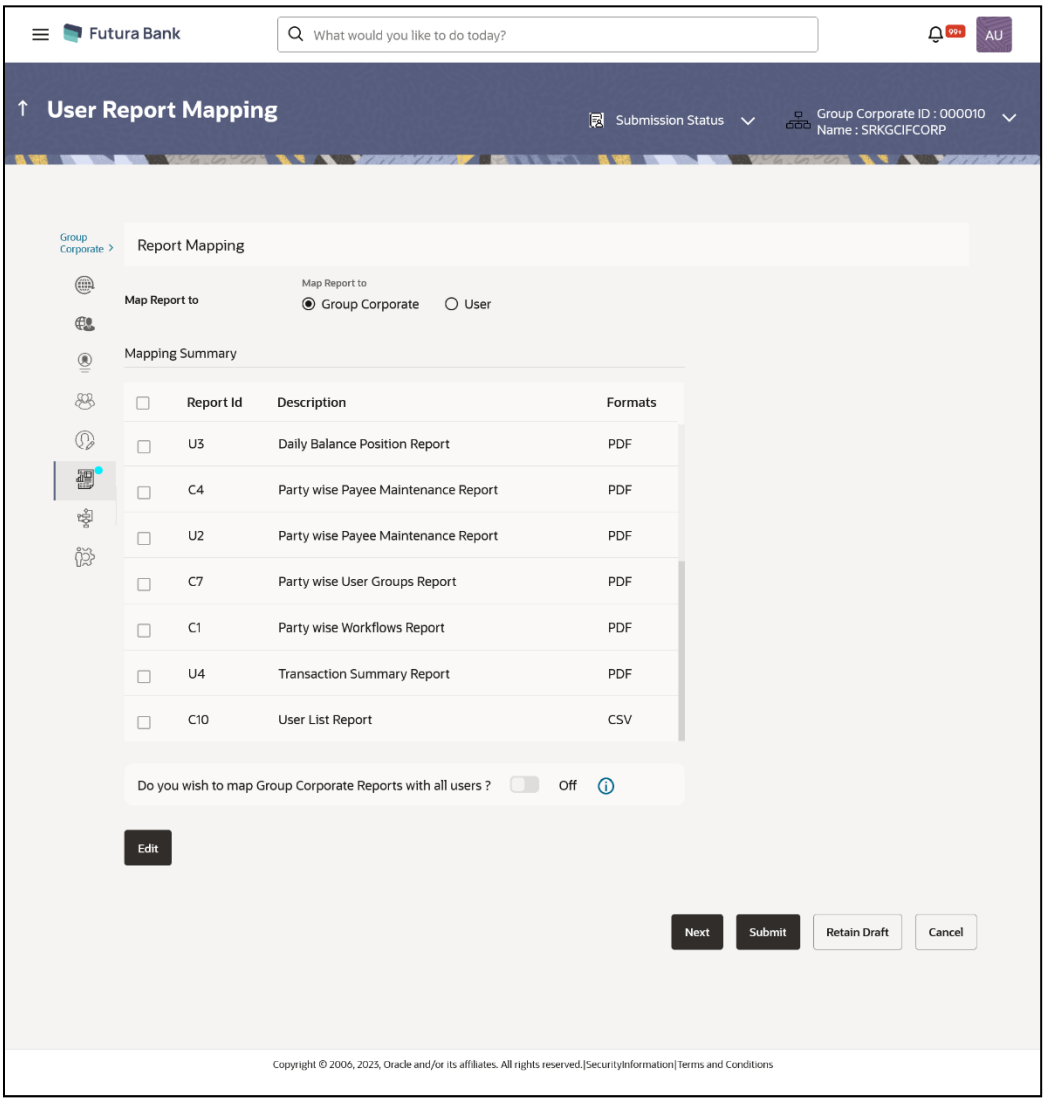
User Report Mapping – Mapping Summary (User Level)



Field Description

Field Name	Description
Map Report to	Select the appropriate option whose mapped reports to be viewed. The options are: • Group Corporate • User
Below fields appears if you select **User** option in the **Map Report to** field.	
User ID	To search the user with the user ID. Partial search is allowed.
First Name	To search the user with the user first name. Partial search is allowed.
Last Name	To search the user with the user last name. Partial search is allowed.
Email	To search the user with the email address of the user. Partial search is allowed.
Mobile Number	Allows to search based on mobile number of the user. Partial search is allowed. Note: Select international subscriber dialing (ISD) code along with the mobile number to search the user.
Party ID	To search the user with the party ID. Partial search is allowed.
Search Result	
Initials	The initials of the user.
User Name	User name of the corporate user.
Full Name Details	The full name of the corporate user.
Mapping	Displays whether the file identifier is mapped to the user. • - denotes that the report is mapped to the user • - denotes that the report is not mapped to the user.

User Report Mapping – Mapping Summary (Group Corporate Level)



Field Description

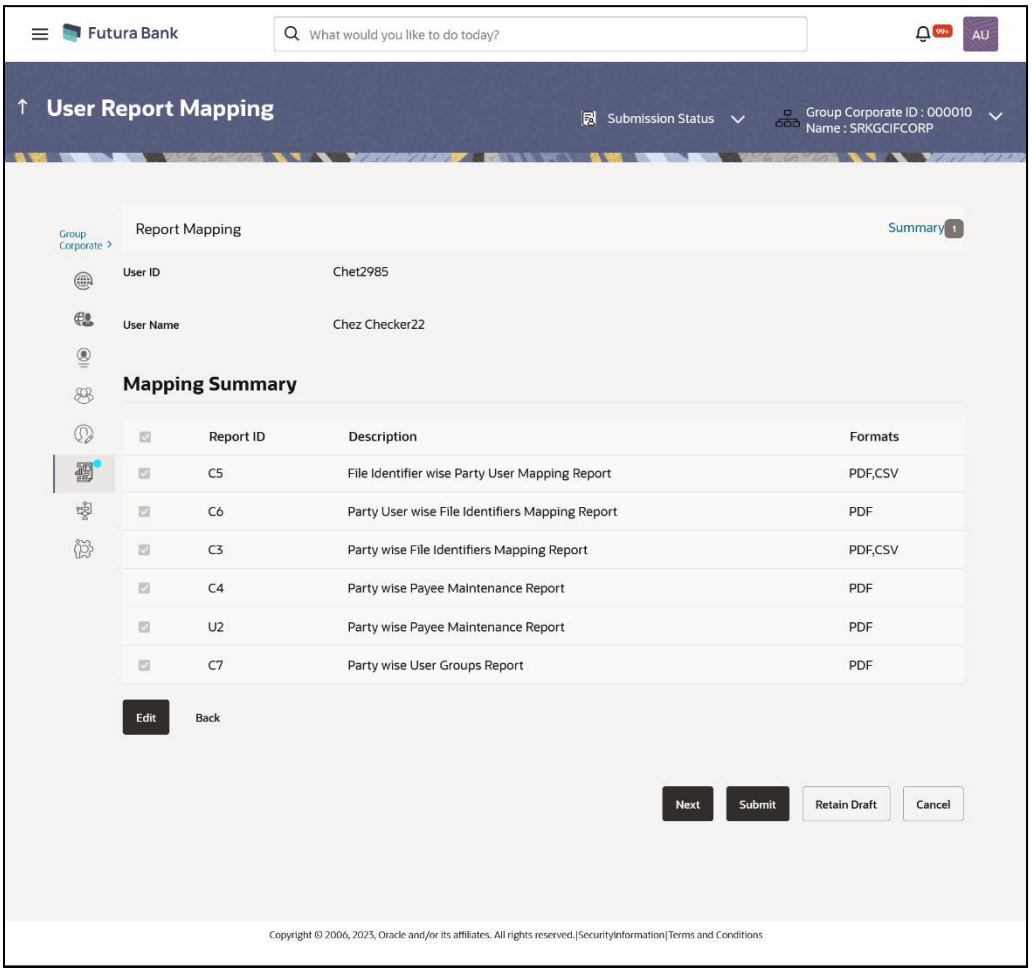
Field Name	Description
Map Report to	Select the appropriate option whose mapped reports to be viewed. The options are: • Group Corporate • User

Mapping Summary

Field Name	Description
Report ID	Unique id assigned to the mapped report.
Description	Description of the report.
Formats	Formats in which a report can be generated.

2. Click against the record for which you want to view the details. The **User Report Mapping - View** screen appears.

User Report Mapping – View



Field Description

Field Name	Description
User Name	Name of the corporate user.
User ID	User ID of the corporate user.
Mapping Summary	
Report ID	Unique id assigned to the mapped report.
Description	Description of the report.
Formats	Formats in which a report can be generated.

3. Click **Edit** to update the user report mapping.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.

15.7.2 User Report Mapping - Create

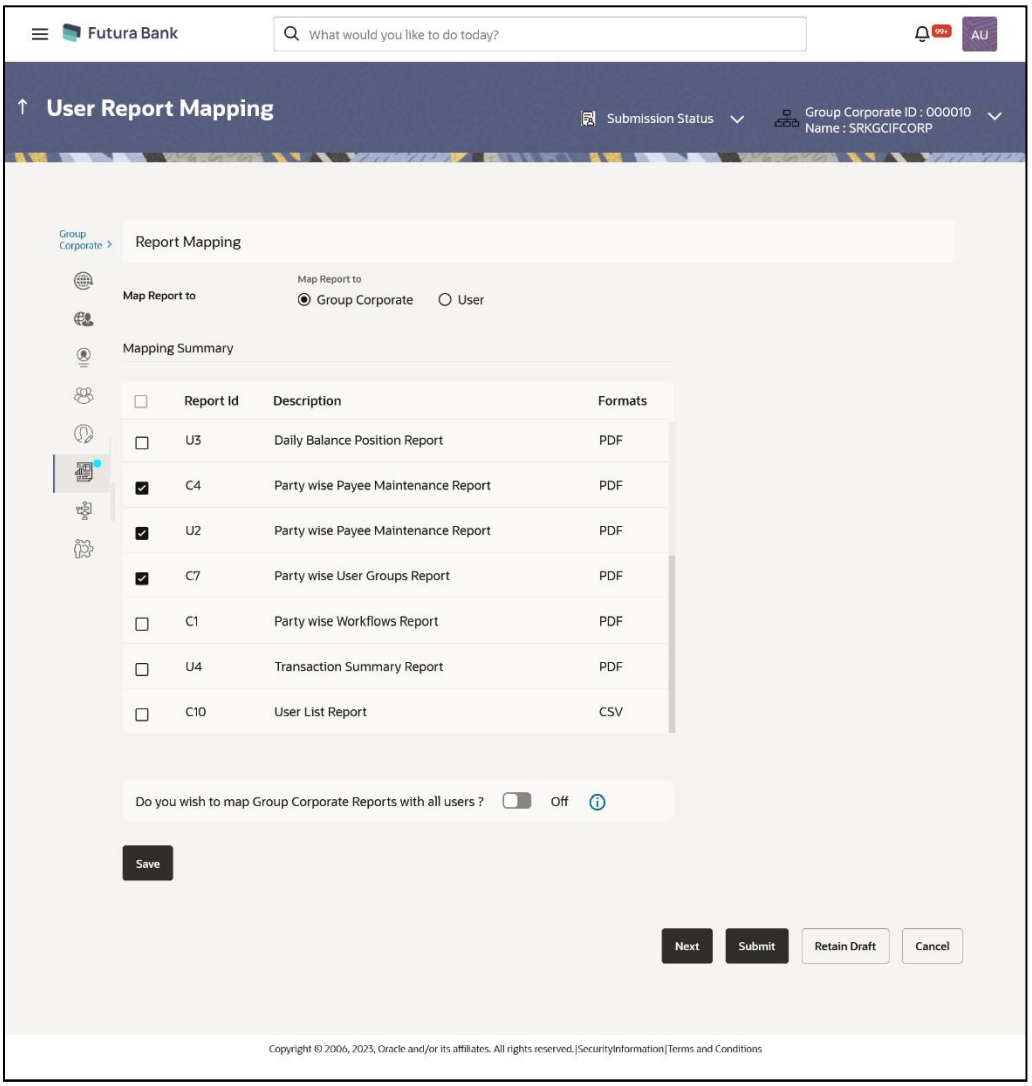
Using this option Bank Administrator can map the reports to a specific corporate user.

To map the reports to a user:

1. Enter the search criteria, click **Search**. The **User Report Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.

2. Click of user record, for which you want to map the report/ s. The **User Report Mapping** screen to create the report mapping appears.

User Report Mapping - Create



Field Description

Field Name	Description
User Name	Name of the corporate user.
User ID	User ID of the corporate user.
Mapping Summary	
Report ID	Unique id assigned to a report.

Field Name	Description
Description	Description of the report.
Formats	The format in which the report is to be generated. The format could be PDF, XLSX.

3. In the **Mapping Summary** section, select the report id of the report which you want to map to the user.
4. Click **Save** to save the maintenance, and redirect to the review page.
   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.
5. The **Review** screen appears. Verify the details, and click **Confirm**.
4. OR
   Click **Add Another** to add another maintenance of the same step.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
6. The success message appears along with the transaction reference number and status of the transaction.

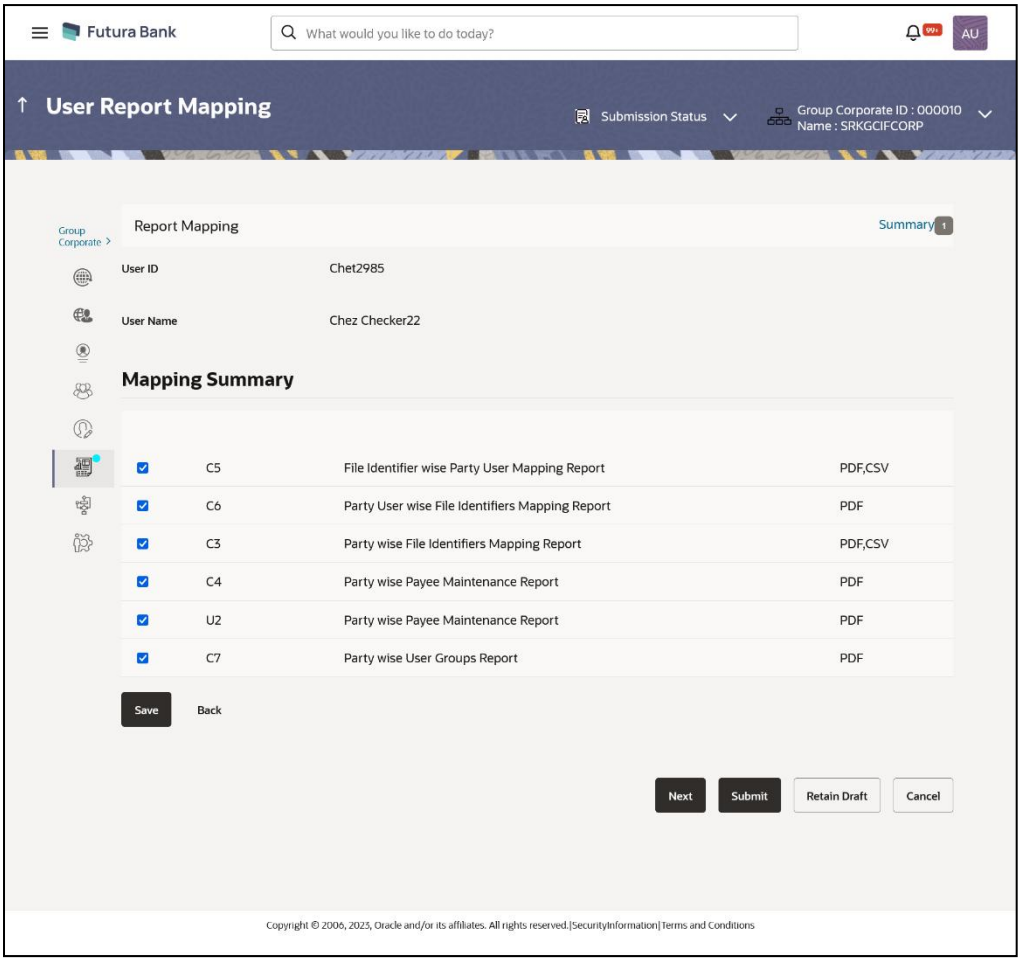
15.7.3 User Report Mapping - Edit

Using this option Bank Administrator can edit the mapping or un-map the reports from specific corporate user.

To edit a User Report Mapping:

1. Enter the search criteria, click **Search**. The **User Report Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.
2. Click against the record for which you want to view the details. The **User Report Mapping - View** screen appears.
3. Click **Edit**. The **User Report Mapping - Edit** screen appears.

User Report Mapping - Edit



4. View the details of report mapping already saved. Select or de-select the report id record to map / un-map a report to a user.
5. Click **Save** to save the modified details.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
7. The success message appears along with the transaction reference number and status of the transaction.

15.8 Step 7: Workflow Management

Approval workflows are created to support requirements where multiple levels of approval are required in a specific sequence for a transaction/maintenance. Each workflow can be configured to have up to five levels of approval with a specific user or a user group configured at each level. The number of levels can be configured.

Workflows can be configured for approval as well as release.

Workflows can be created independently and can be attached to a specific transaction/maintenance as part of the Approval Rule configuration.

The approver is responsible for giving formal authorization to proceed with a transaction. The approver decides to approve or reject the transaction based on its validity and compliance with regulations.

The checker is responsible for verifying the accuracy and completeness of the transaction details before they are approved or released. The checker reviews supporting documents and ensures all information is correct and complete.

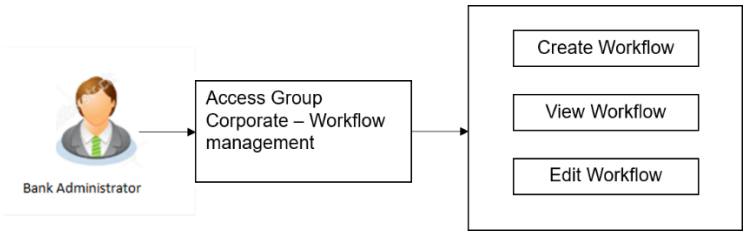
The releaser is responsible for the final step of authorizing and executing the transaction, often after it has been checked and approved. The releaser initiates the actual release of funds or completion of the transaction.

Workflow Type: The workflow can be created for Approval or Release types of flows.
Within the '**Approval'** workflow type, user can configure either an approver or checker at each level. The Approval workflow can be setup with a specific user or a user group configured at each level. The number of levels is configurable for 'Approval' workflow type. There is no restriction on the count of checkers/approvers within an 'Approval' workflow type.
Within the '**Release'** workflow type, user can configure a releaser workflow. The Release workflow can be setup with a specific user or a user group configured at a single level. Only 1 level can be configured for 'Release' workflow type.

Prerequisites

- Transaction access is provided to Bank Administrator.
- Party preference is maintained.
- Multiple users are maintained under a party or as Bank Administrators
- Approval rule set up for Bank Administrator to perform the actions.
- Necessary user groups are maintained using User Group Management.

Workflow



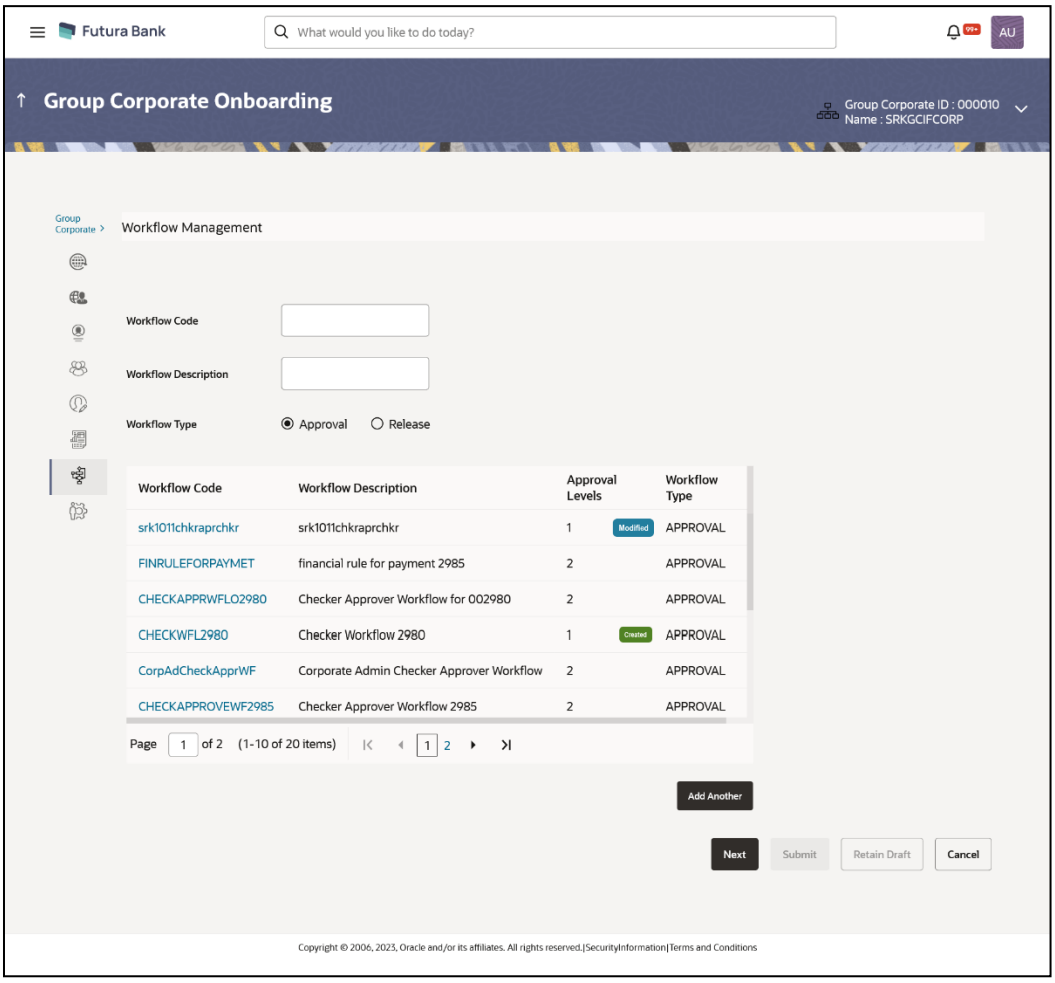
How to reach here:

System/ Bank Administrator Dashboard > Corporate Onboarding > Group Corporate Onboarding > Workflow Management tab
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Group Corporate Onboarding > Workflow Management tab

15.8.1 Workflow Management – Summary

User can opt to view the details of existing workflows or can create new approval workflow using this screen based on the choose workflow type

Workflow Management – Summary



Field Description

Field Name	Description
Workflow Code	Enter the approval workflow code to be searched.
Workflow Description	Enter the description of the approval workflow to be searched.
Workflow Type	Specify the workflow type to be searched. The options are: • Approval • Release
Search Result	
Workflow Code	Code of the already maintained approval workflow. This field will be displayed only if there are existing approval workflows available.
Workflow Description	Description of the already maintained approval workflow. This field will be displayed only if there are existing approval workflows available.
Approval Levels	Number of approval levels in each workflow. This field will be displayed only if there are existing approval workflows available.
Workflow Type	Displays the type of workflow whether it is for Approval or Release.

1. In the **Workflow Code** field, enter the approval workflow code to be searched.
2. In the **Workflow Description** field, enter the description of the approval workflow to be searched.
3. In the **Workflow Type** field, select the type of workflow to be searched.
4. Click **Search**. The **Workflow Management** screen with search results appears based on the searched criteria.
5. Click the **Workflow Code** link to view details of the selected Approval Workflow. The **Workflow Management - View** screen appears.
   OR
   Click **Create**. The **Workflow Management - Create** screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to go back to previous screen.

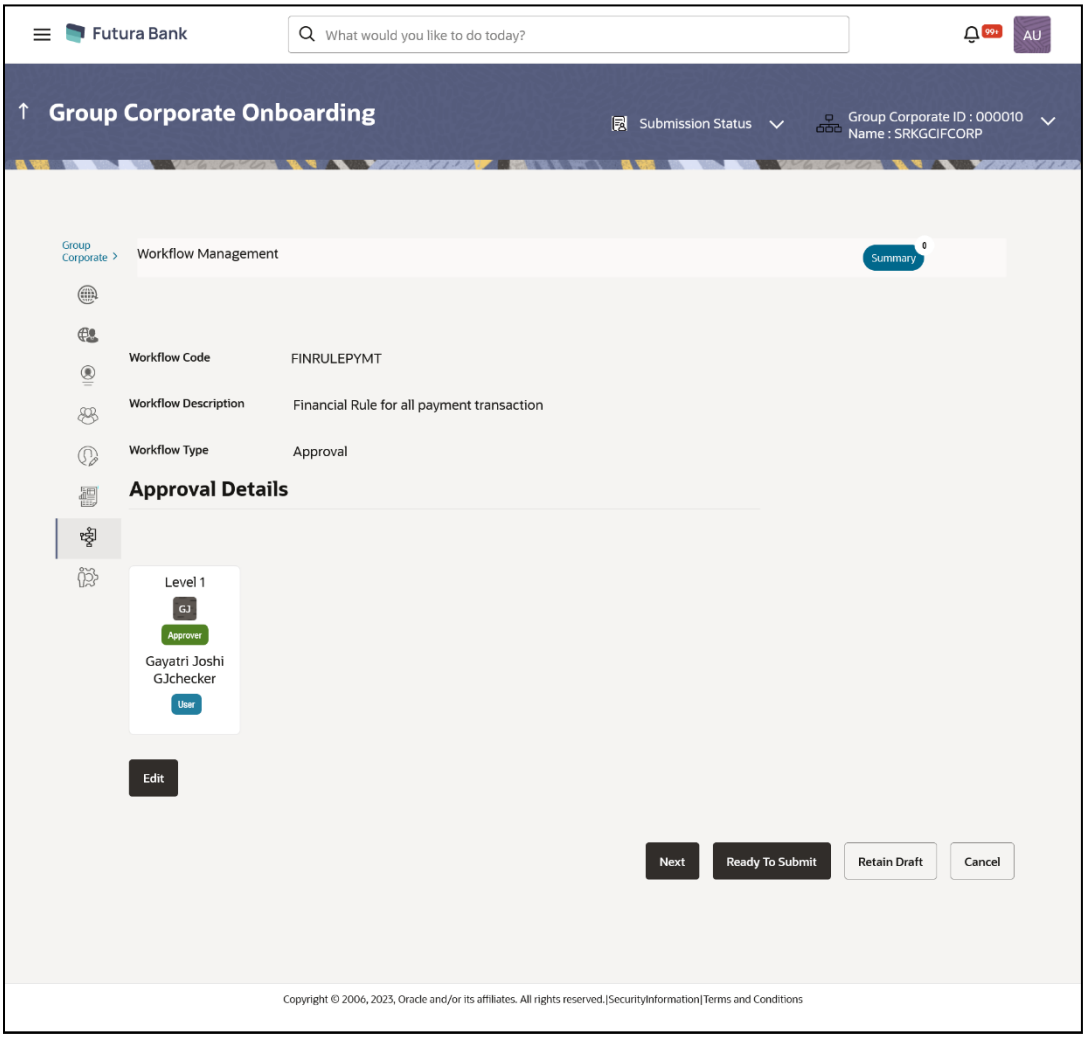
15.8.2 Workflow Management –View

Further drill down is provided on each workflow to view the details of the users/ user groups who are a part of the workflow

To view the approval workflow for corporate users:

1. In the **Workflow Management** screen, enter the search parameters and click **Search**. The **Workflow Management** screen with search results appears based on the searched criteria.
2. Click the **Workflow Code** link to view details of the selected Approval Workflow. The **Workflow Management - View** screen appears.

Workflow Management – View



Field Description

Field Name	Description
View	
Workflow Code	Workflow code is displayed.
Workflow Description	Workflow description is displayed.
Workflow Type	The type of workflow i.e. whether it is for approval or release.
Approval Details	
Approval Level	User / user group maintained at each approval level.
User / User Group	User or a user group maintained at each level of approval. On Approval -Workflow screen, Admin User can click on the Name of the user group that is part of the workflow to see the list of users which are part of that Group. User can search specific user name, by using the search window on Group Details overlay.
Release Details	
User / User Group	Displays the user or a user group maintained to release the transaction.

3. Click **Edit** to edit the workflow. The **Workflow Management - Edit** screen with values in editable form appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.

15.8.3 Workflow Management – Create

Bank Administrator can create approval workflows for corporate users. By default, user can specify minimum one and maximum five levels of approvals as a part of workflow.

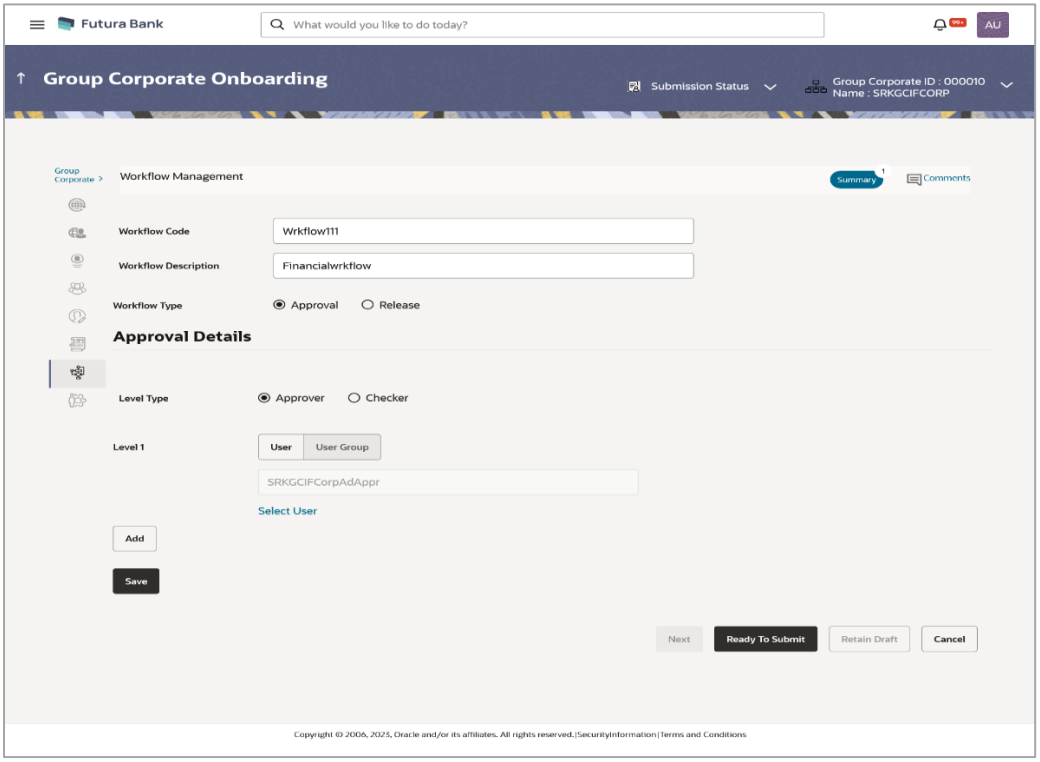
Bank admin can also create workflow for release if the Release Facility is enabled at Group Corporate Level. Admin can specify user or user group who will release the transaction. All the users and user groups created under the Corporate Group will be made available for mapping.

If level type is Approver, the user can provide multiple levels within the workflow. Each level can be specified as an Approver or Checker and for each level (approver or checker), the type can be selected as User or User Group.

Note:
1) Release functionality can be configured only for corporate user's transactions.
2) Only one level of releaser can be configured in the workflow.
3) The same user can act on the same transaction only once in a particular role (checker or approver). For example, the same user can check the same transaction only once as a checker.
4) The bank needs to operationally ensure that approver levels are also added. If only checkers are added and no approver is added, then the transaction will be processed without an approver.

Administrator can set either an individual user or user group of a corporate as part of each approval level. Approval type (sequential/non-sequential/no authorization) is defined at the party preference.

Workflow Management – Create



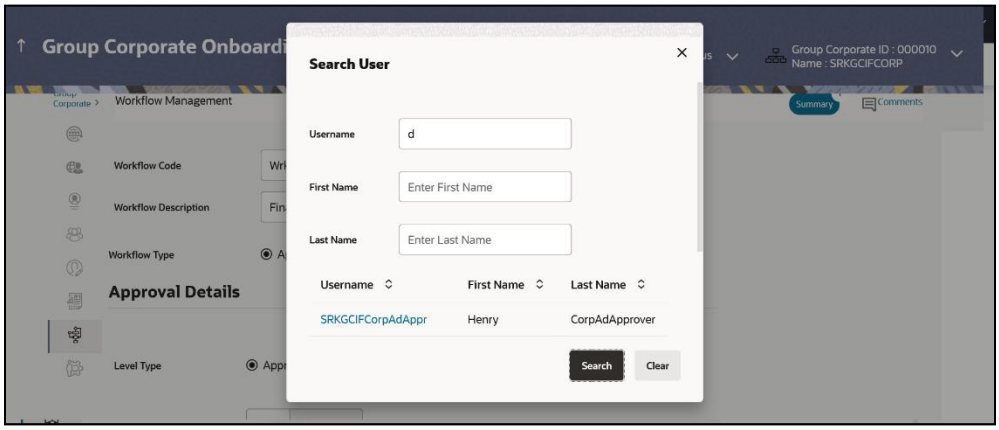
Field Description

Field Name	Description
Create	
Workflow Code	To specify approval workflow code.
Workflow Description	To specify approval workflow description.
Workflow Type	Specify whether the workflow which the administrator is creating are for approval or for release functionality. The options are: • Approval • Release
Approval Details	
Below fields appears if you select **Approval** option in the **Workflow Type** field.	
Level Type	Specify the level type for the workflow. The options are: • Approver • Checker
Level	Approval levels for a user / user group. User can click Add for multi-level approval process.
User / User Group	To select specific user or a user group at each level of approval. Note: All the users and user groups created under the Group Corporate will be made available for mapping.
Release Details	
Below fields appears if you select **Release** option in the **Workflow Type** field.	
User / User Group	To select specific user or a user group to release the transaction. Note: 1) All the users and user groups created under the Group Corporate will be available for mapping. 2) Only one level of releaser can be configured in the workflow.

To create an approval workflow:

1. Click on the **Add Another** to create new create approval workflows for corporate users. The **Workflow Management – Create** appears.
2. In the **Workflow Code** field, enter the workflow code.
3. In the **Workflow Description** field, enter the name of the workflow.
4. If you have selected **Approval** option in the **Workflow Type** field;
   a. In the **Level Type** field, specify the level type for workflow.
   b. In the **Level 1** field, select the appropriate user / user group in the **Approval Details** section.
   c. Click icon to add appropriate user / user group.
   The **User Search** popup appears. All the users and User groups created under the Group Corporate will be available for assigning at various approval levels.

Workflow Management – User Search



Field Description

Field Name	Description
Search	
User Name	To search the user with the user name. Partial search is allowed.
First Name	Allows to search based on first name or given name of the user.
Last Name	Allows to search based on last name/ surname of the user.
Search Results	
User ID	User ID of the user.

Field Name	Description
Full Name	Full Name of the user.
Last Name	Last Name of the user

d. From the **User Name / User Groups** list, click & select the approver user name at specific level of approval.
OR
Click icon to remove user/ user group.

e. Click **Add** to add the selected user/ user group at specific level of approval.
OR
Click icon to remove specific approval level.

5. If you have selected **Release** option in the **Workflow Type** field;

a. In the **Level 1** field, select the appropriate user / user group in the **Approval Details** section.

b. Click icon to add appropriate user / user group.
The **User Search** popup appears. All the users and User groups created under the Group Corporate will be available for assigning at various approval levels.

6. Click **Save** to save Approval Workflow.
OR
Click **Back** to navigate back to previous screen.
OR
Click **Next** to proceed to the next logical step.
OR
Click **Submit** to submit the steps performed so far for approval.
OR
Click **Retain Draft** to save the details entered as draft.
OR
Click **Cancel** to cancel the transaction.

7. Click **Edit** to modify the details entered.
OR
Click on **Add Another** to new Workflow.
OR
Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate back to previous screen.

8. The success message of saving the created approval workflow appears along with the transaction reference number and status.

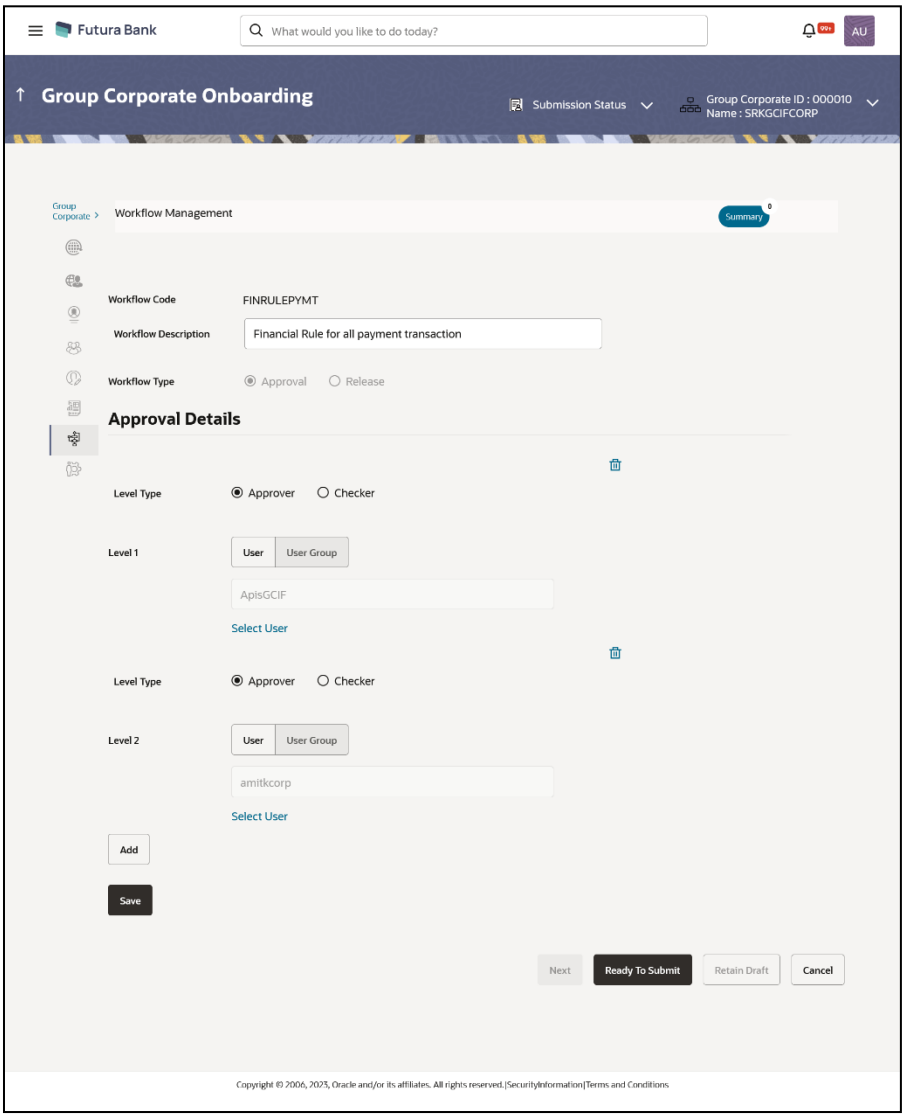
15.8.4 Workflow Management - Edit

This function enables the Bank Administrator to update the description of the workflow and also to remove existing and add new approval levels. Edited workflows are applicable for new transactions initiated post workflow update, whereas the previously initiated and pending approval transactions pending will follow the old workflow.

To edit an approval workflow:

1. In the **Workflow Management** screen, enter the search parameters and click **Search**. The **Workflow Management** screen with search results appears based on the searched criteria.
2. Click the **Workflow Code** link to view details of the selected Approval Workflow. The **Workflow Management - View** screen appears.
3. Click **Edit** to edit the workflow. The **Workflow Management - Edit** screen with values in editable form appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to the previous screen.

Workflow Management - Edit



Field Description

Field Name	Description
Edit	
Workflow Code	Workflow code is displayed.
Workflow Description	Workflow description is displayed in editable form.

Field Name	Description
Workflow Type	Specify whether the workflow which the administrator is creating are for approval or for release functionality. The options are: • Approval • Release
Approval Details	
Below fields appears if you select **Approval** option in the **Workflow Type** field.	
Level Type	Specify the level type for the workflow. The options are: • Approver • Checker
Level	Approval levels for a user / user group. Administrator can remove or add approval levels in a workflow. This is editable field.
User Name / User Groups	User or a user group maintained at each level of approval. Administrator can edit an existing user/user group maintained at each level and can also specify user/user group for additional approval level. This is editable field.
Release Details	
Below fields appears if you select **Release** option in the **Workflow Type** field.	
User / User Group	To select specific user or a user group to release the transaction. This is editable field. Note: All the users and user groups created under the Group Corporate will be made available for mapping.

4. Edit the required details.
5. Click **Add** to add the selected user/ user group at specific level of approval.
   OR
   Click icon to remove specific approval level.

6. Click **Save** to save Approval Workflow.
   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.
7. Click **Edit** to modify the details entered.
   OR
   Click on **Add Another** to add new Workflow.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
8. The success message of saving the approval workflow modification appears along with the transaction reference number and status.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

15.9 Step 8: Approval Rules

This function enables the Bank Administrator to set up conditions for approval as well as for Releaser as per the bank/corporate requirements. A rule can be set up for financial, non-financial, non-account financial transactions and for maintenances. Flexibility is provided to define approval rules with conditions stating that 'specific transaction' if initiated by a 'specific user/ user group/All users' has to be approved by a 'specific approver/approver group' along with other attributes like amount range etc.

For an approval rule, the user has an option to select one workflow within which different levels are available for approver and checker. The release rules should be resolved at the time of transaction initiation. The users mapped at the time of transaction initiation will be able to release the transaction. The rules specific to release can be configured for a combination of initiator type (user, user group), transactions and accounts. User can set up the release rule only for those transactions for which the release functionality is required. If no rule is configured for a combination of values, then it will be considered as 'no release required'. All the transactions as per the specified rule, will be sent for release to the configured users/user groups post successful approval at all levels.

Prerequisites:

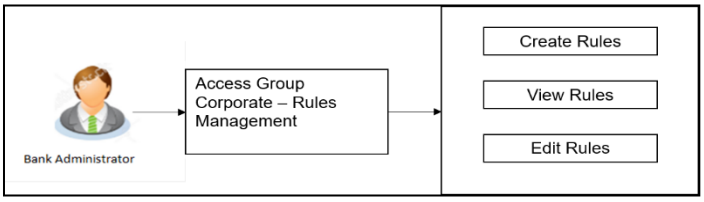
- Transaction access is provided to Bank Administrator
- Party preference is maintained for setting up rules for corporates
- Corporate and Administrator users are maintained
- Workflow configuration is maintained if approval required is to be set as 'Yes'
- Approval rule set up for Bank Administrator to perform the actions
- Necessary user groups and approval workflows are maintained

Features supported in application

The Approval Rule maintenances allow the bank administrator to:

- Create Approval Rules
- View Approval Rules
- Edit Approval Rules
- Delete Approval Rules

Workflow



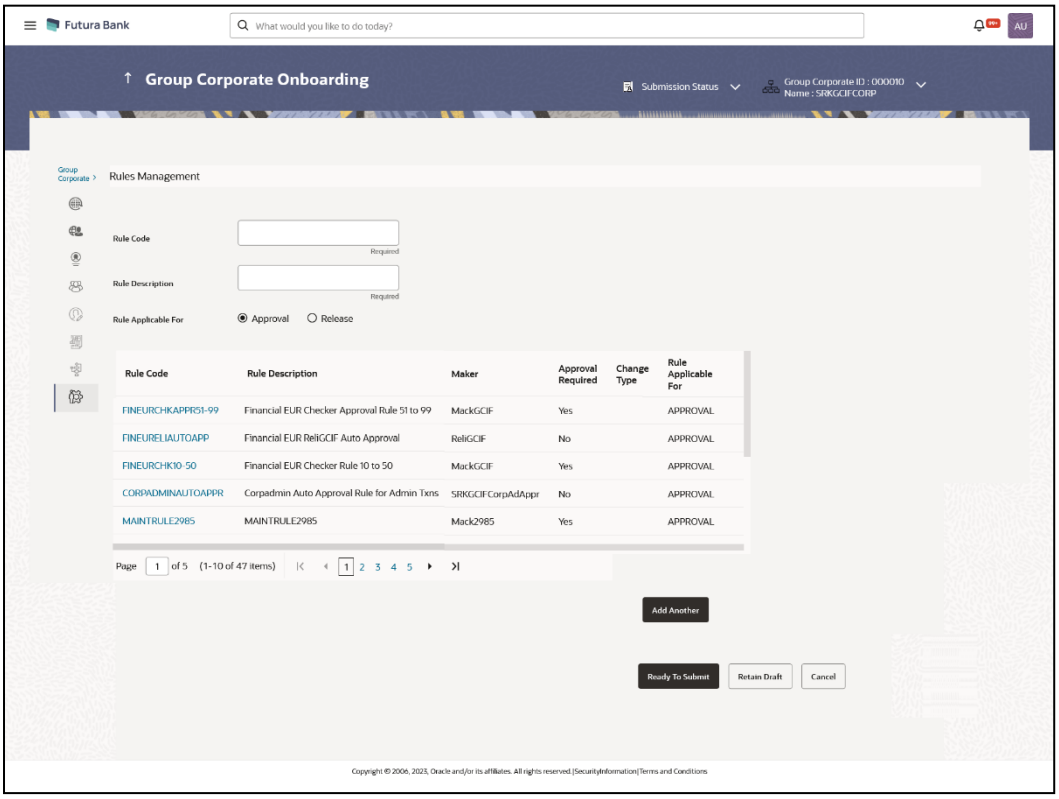
How to reach here:

System/ Bank Administrator Dashboard > Corporate Onboarding > Group Corporate Onboarding > Approval Rules tab
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Group Corporate Onboarding > Approval Rules tab

15.9.1 Approval Rules – Summary

Bank Administrator logs into the system and navigates to the Rules Management screen. User can opt to view the details of existing Approval Rules or can create new approval rule using this screen.

Rules Management – Summary



Field Description

Field Name	Description
Rule Code	Search with Approval rule code.
Rule Description	Search with Approval rule description.
Rule Applicable For	Search whether rule is applicable for Release or Approval.
Search Result	
Rule Code	The Approval rule code.
Rule Description	The Approval rule description.
Maker	Initiator type (User ID or User Group Code) of the transaction. This field will be displayed only if existing approval rules are available.

Field Name	Description
Approval Required	Whether approval is required for each rule maintained.
Change Type	Displays the status of the record i.e. if it is created or modified.
Rule Applicable for	Displays the whether the approval rule is applicable for Release or Approval.

1. In the **Rule Code** field, enter the approval Rule code to be searched.
2. In the **Rule Description** field, enter the description of the approval Rule to be searched.
3. In the **Rule Applicable For** field, specify whether the approval rule is applicable for Release or Approval.
4. Click **Search**. The **Rule Management** screen with search results appears based on the searched criteria.
5. Click the **Rule code** link, to view details of the selected Approval Rule. The **Approval Rules - View** screen appears.
   OR
   Click on **Add Another** to add the **Approval Rules.**
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to previous screen.
   OR
   Click **Create** to create new Approval Rule for corporate users.

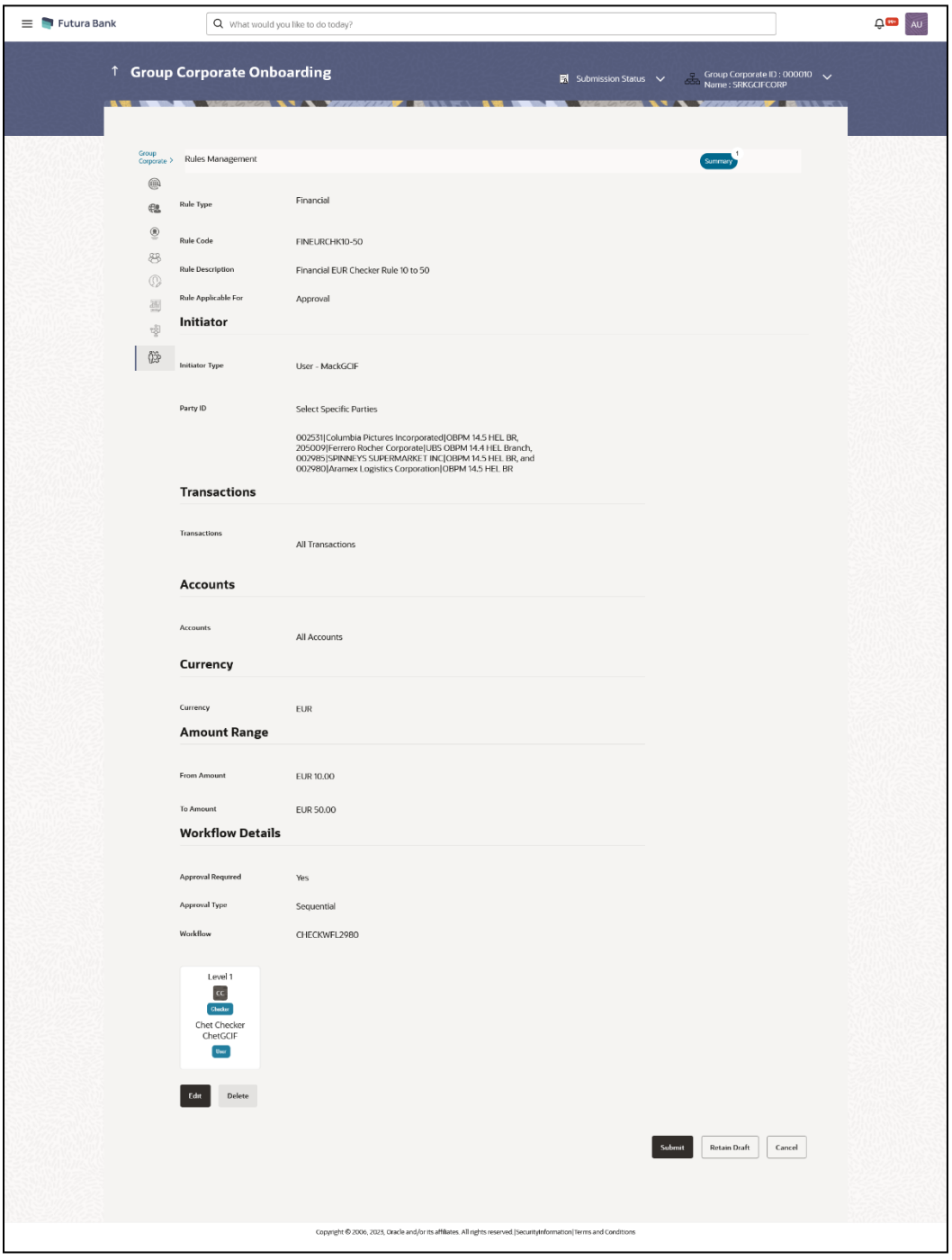
15.9.2 Approval Rules - View

On accessing 'Rules Management' menu option, and searching rules, summarized view of all the approval rules maintained (if any) for the party are displayed on the screen. Further drill down is given on each rule to view the details of approval rule.

To view the approval rules for corporate users:

1. In the **Approval Rules** screen, enter the search parameters and click **Search**. The **Approval Rules** screen with search results appears based on the searched criteria.
2. Click the **Rule Code** link, for which you want to view the details. The **Approval Rules - View** screen appears.

Approval Rules View



Field Description

Field Name	Description
View	
Rule Type	Transaction rule type for which the approval rule is set up. The transaction rule for corporate user are: • Financial • Non Financial • Maintenance • Non Account Financial • Administration • Service Request
Rule Code	Approval rule code.
Rule Description	Approval rule description.
Rule Applicable For	Displays for which the rule is set up. It could be: • Approval • Releaser
Initiator	
Initiator Type	Initiator type specified while creating a rule. Note : “ All Users’ will be displayed for Initiator Type if rule is created with Initiator type as “All users”
User Name / User Groups	Name of the user or user group defined as initiator for the rule condition.
Party ID	Displays one or multiple Party IDs mapped to the selected Group Corporate ID.

Field Name	Description
Transactions	The transactions for which the rule is being set up. The options are: • All Transactions • Select Specific Transactions • All Service Request – rule will be applicable for all the service requests available in the form builder • Select Specific Category – all the service request categories available in the form builder will be listed for selection where one category can be selected • Select Specific Service Request - all the service requests available in the form builder will be listed for selection where one service requests can be checked Type of transactions available depends on the selection of rule type. The option **'All Service Requests', 'Specific Service Request' or 'Specific Category'** is enabled only if the **Service Request** option is selected in **Rule Type** field.
Accounts	Field will display the accounts along with their names mapped based on the Party ID selection for which rule being viewed is set up. The options are: • All Accounts • Select Specific Accounts This field appears if you select **Financial** and **Non Financial** in the **Rule Type** field.
Currency	Currency type in which the financial approval rule for a corporate is defined. This field appears if you select **Financial** and **Non Account Financial** in the **Rule Type** field. Note: 1) Entity's base currency (maintained in System Configuration) will be defaulted in the currency field. 2) User will be able to select the currency other than the default currency from the currency list.
Amount Range	

Field Name	Description
From Amount/ To Amount	Transactions allowed for the user between the amount range. This field appears if you select Financial and **Non Account Financial** in the Rule Type field.
Workflow Details	
Approval Required	Field displays whether approval is required or not. The options are: • Yes • No
Approval Type	Displays the Approval workflow type. Possible value will be: • Sequential • Parallel This field is displayed if **Yes** option is selected in **Approval Required** field and when workflow preference is set at **Rule Level** in Group Corporate Profiling setup.
Workflow	Field displays the approval workflow details along with the defined approval levels. For release, it displays the release workflow details. This field appears if you select **Yes** in the **Approval Required** field.

3. Click **Edit** to edit the approval rule. The **Approval Rule - Edit** screen with values in editable form appears.
   OR
   Click **Delete** to delete the approval rule.
   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.

15.9.3 Approval Rules - Edit

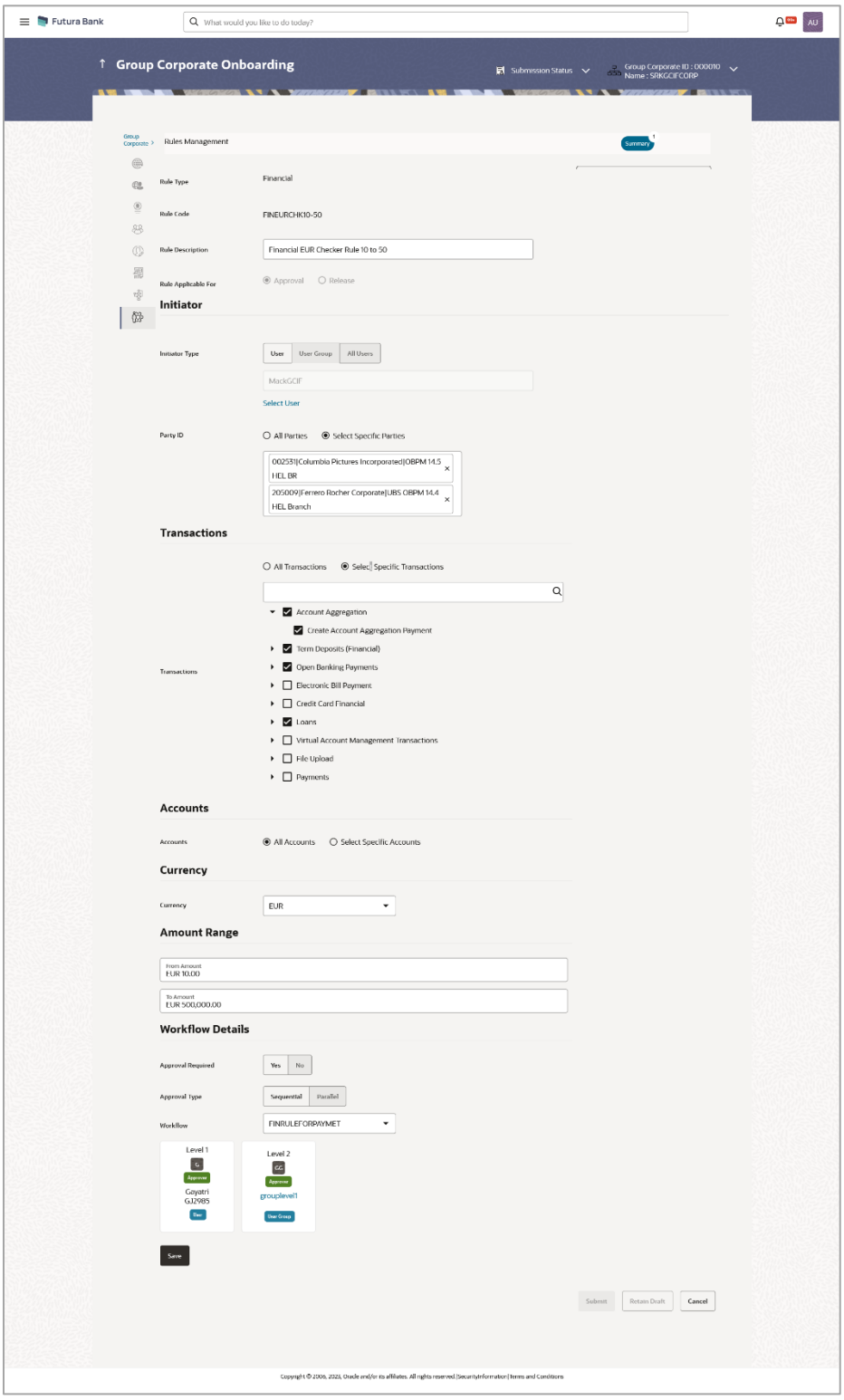
Bank Administrator can edit the approval rules. An administrator is allowed to change the description of the rule and is also allowed to change the parameters associated with the specific approval rule.

Edited rules are applicable for new transactions initiated post rule update. Previously initiated transactions which are pending approval will follow a rule which was applied at the time of transaction initiation.

To edit an approval workflow:

1. In the **Approval Rules** screen, enter the search parameters and click **Search**. The **Approval Rules** screen with search results appears based on the searched criteria.
2. Click the **Rule Code** link, for which you want to view the details. The **Approval Rules - View** screen appears.
3. Click **Edit** to edit the approval rule. The **Approval Rule - Edit** screen with values in editable form appears.

Approval Rules - Edit



Field Description

Field Name	Description
Edit	
Rule Type	Transaction rule type for which the approval rule is set up will be displayed. The rule type cannot be modified. The transaction rule for corporate user are: • Financial • Non Financial • Maintenance • Non Account Financial • Administration • Service Request
Rule Code	Approval rule code provided by the user.
Rule Description	Approval rule description provided by the user in editable form.
Rule Applicable For	The rule applicable for Release or Approval in editable form. The rule applicable for cannot be modified
Initiator	
Initiator Type	Initiator type who initiates the transaction will be displayed in editable form. **Note**: If 'All Users' is selected, then the rule being created is applicable for all users of Corporate Party
User Name / User Groups	Name of the user or user group as initiator will be displayed in editable form. If initiator is selected as User, then all the users belonging to the party will be listed for selection. If initiator is selected as User Group, then all the user groups belonging to the party will be listed for selection.
Party ID	The one or multiple Party IDs mapped to the selected Group Corporate ID will be displayed in editable form.

Field Name	Description
Transactions	The transactions to set the approval rules will be displayed in editable form. The options are: • All Transactions – If selected, the rule can be setup for all transactions • Select Specific Transactions – Specific transactions can be selected for which the rule is applicable. The transaction type and names are listed for selection • All Service Request – rule will be applicable for all the service requests available in the form builder • Select Specific Category – all the service request categories available in the form builder will be listed for selection where one category can be selected • Select Specific Service Request - all the service requests available in the form builder will be listed for selection where one service requests can be checked Type of transactions available depends on the selection of rule type. The option **'All Service Requests', 'Specific Service Request' or 'Specific Category'** is enabled only if the **Service Request** option is selected in **Rule Type** field.
Accounts	Type of accounts based on the Party ID selection will be displayed in editable form. The options are: • All Accounts – If selected, the rule can be setup for all accounts within the selected Party IDs • Select Specific Accounts – Specific accounts can be selected for which the rule is applicable. The Party ID, Account Type and Account Numbers along with their names are listed for selection This field appears if you select **Financial** and **Non Financial** in the **Rule Type** field.
Currency	Currency type in which the financial approval rule for a corporate is defined.
Amount Range	

Field Name	Description
From Amount/ To Amount	Transactions allowed for the user between the defined amounts ranges will be displayed in editable form. This field appears if you select **Financial and Non Account Financial** in the **Rule Type** field.
Workflow Details	
Approval Required	Whether approval is required will be displayed in editable form. The options are: • Yes • No
Approval Type	Define the Approval workflow type. Possible value will be • Sequential • Parallel This field is enabled if **Yes** option is selected in **Approval Required** field and when workflow preference is set at **Rule Level** in Group Corporate Profiling setup.
Workflow	Details of the approval workflow within which different levels are available for approver and checker will be displayed in editable form. For release, it displays the release workflow details. This field appears if you select **Yes** in the **Approval Required** field.

4. Edit the required details.
5. Click **Save** to save the approval rule.
   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click **Next** to proceed to the next logical step.
   OR
   Click **Submit** to submit the steps performed so far for approval.
   OR
   Click **Retain Draft** to save the details entered as draft.
   OR
   Click **Cancel** to cancel the transaction.
6. The **Approval Rule - Edit Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click on **Add Another** to add new Rule.

OR
Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate back to previous screen.

7. The success message of saving the approval rule modification appears along with the transaction reference number and status.
Click **OK** to complete the transaction and navigate back to 'Dashboard'.

15.9.4 Approval Rule – Create

Bank Administrator can create approval rules for the corporate users. In Approval Rules, Bank Administrator can define the rule conditions for various type of transactions.

Approval rules can be setup based on the following parameters.

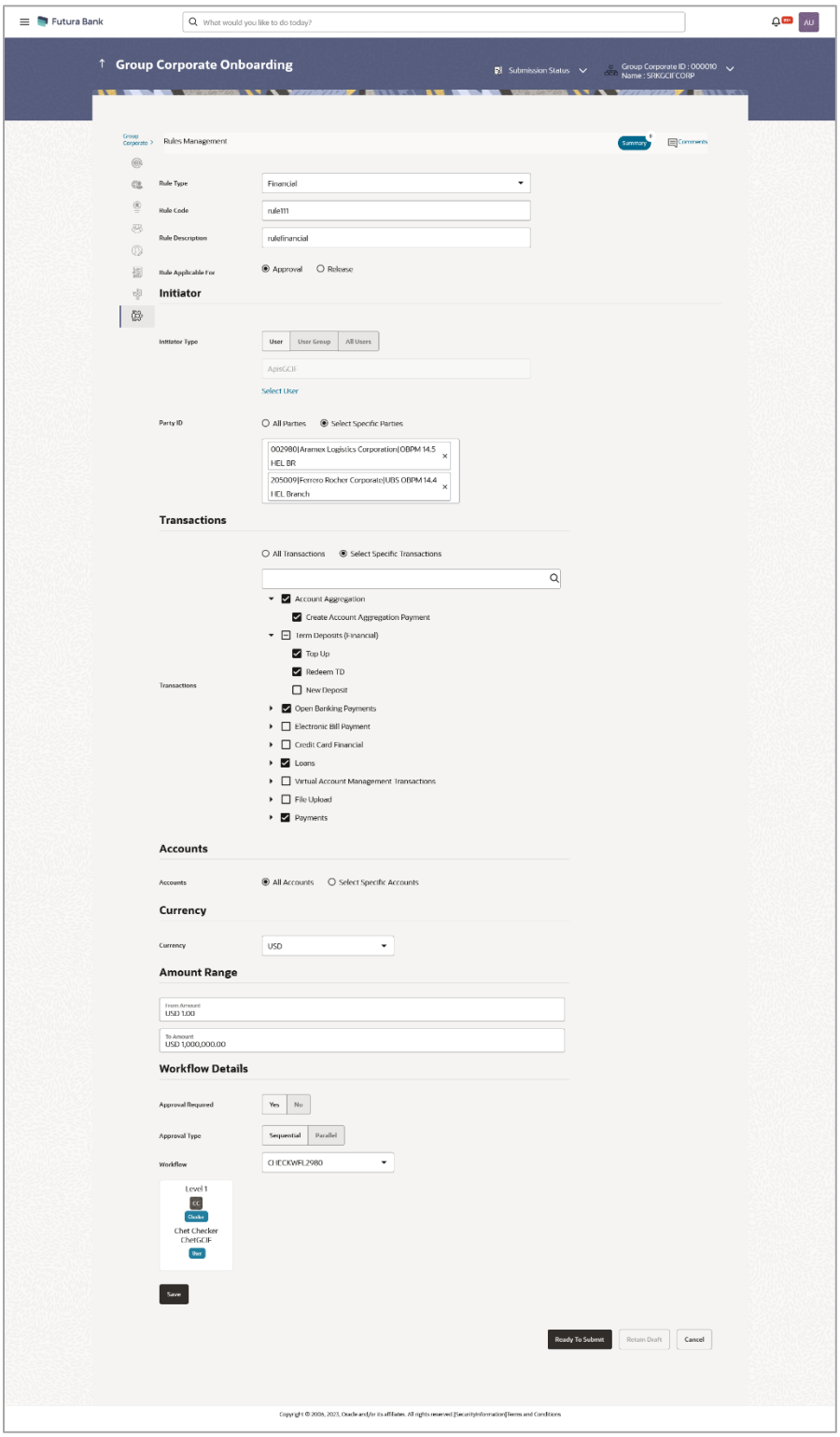
- Type of Transaction
  - Financial Transactions
    - This option is used to setup approval rules for the transactions, this involves exchange of money.
    - E.g. Money Transfer, Draft Issuance, Redeem Term Deposit etc.
  - Non Financial Transactions
    - This option is used to setup approval rules for the transaction which are for an account but does not involve exchange of money.
    - E.g. Cheque Book Request, Statement Request, Stop Cheque etc.
  - Maintenance
    - This option is used to setup approval rules for the transaction which are at the party level and not for a specific account
    - E.g. Payee Maintenance, Biller Maintenance etc.
  - Non Account Financial Transactions:
    - This option is used to setup approval rules for the transaction with amount range and no debit account
    - E.g. Initiate LC, Supply Chain Finance related transactions like create Invoice.
  - Initiator
    - Specific User
    - User Group
    - All Users
  - Party ID
    - This option allows to select one or multiple Party IDs
  - Accounts
    - All Accounts based on party selection
    - Select Specific Accounts based on party selection

- Transactions
  - All Transactions
  - Select Specific Transactions
- Currency
- Amount Range
- Service Requests
  - All Service Requests
  - Specific Service Request

Specific Category Administrator can create multiple approval rules for corporate users. In a scenario when a transaction is initiated and multiple rules are applicable as per set conditions, then the most applicable rule amongst all the resolved rules is applied for approval.

User can further define if for a condition, the transactions should be auto approved (which means there is no approval workflow and the transactions gets approved as soon as initiator submits the transactions) or should follow a set approval workflow and should get approved by the defined set of approvers. The same is achieved by attaching a workflow maintained for the corporate party.

Approval Rules – Corporate User - Create



Field Description

Field Name	Description
Rule Type	Transaction rule type for which the approval rule needs to be set up. The transaction rule for corporate user are: • Financial • Non Financial • Maintenance • Non Account Financial • Administration • Service Request
Rule Code	To specify approval rule code.
Rule Description	To specify approval rule description.
Rule Applicable For	Specify the rule applicable for Release or Approval. The options are: • Approval • Release
Initiator	
Initiator Type	Initiator type who initiates the transaction. The options are: • User - For creating an approval rule for a single user. A lookup will be provided to search for a specific user • User Group - For creating an approval rule for a User Group • All Users - For creating an approval rule of all the users of the Group Corporate
User / User Group	Name of the user or user group as initiator. If initiator is selected as User, then all the users belonging to the party will be listed for selection. If initiator is selected as User Group, then all the user groups belonging to the party will be listed for selection. If Initiator is selected as 'All Users', then the rule being created is applicable for all users of Corporate Party.

Field Name	Description
Party ID	The one or multiple Party IDs to be mapped to the selected Group Corporate ID.
Transactions	Select the transactions for which the rule is being set up. The options are: • All Transactions – Allow to select all the transactions within module • Select Specific Transactions – Allow to select specific transactions within each module • All Service Request – rule will be applicable for all the service requests available in the form builder • Select Specific Category – all the service request categories available in the form builder will be listed for selection where one category can be selected • Select Specific Service Request - all the service requests available in the form builder will be listed for selection where one service requests can be checked Type of transactions available depends on the selection of rule type. The option **'All Service Requests', 'Specific Service Request' or 'Specific Category'** is enabled only if the **Service Request** option is selected in **Rule Type** field.
Accounts	Specify the accounts mapped based on the Party ID selection for which rule being viewed is set up. The options are: • All Accounts - Allow to select all the accounts of the selected Party ID • Select Specific Accounts - Allow to select specific accounts within each party ID Based on the Party ID selection, accounts associated to the party ID are available for selection. This field appears if you select **Financial** and **Non Financial** in the **Rule Type** field.
Counts of Accounts Mapped	Displays the number of accounts mapped to the Group Corporate.

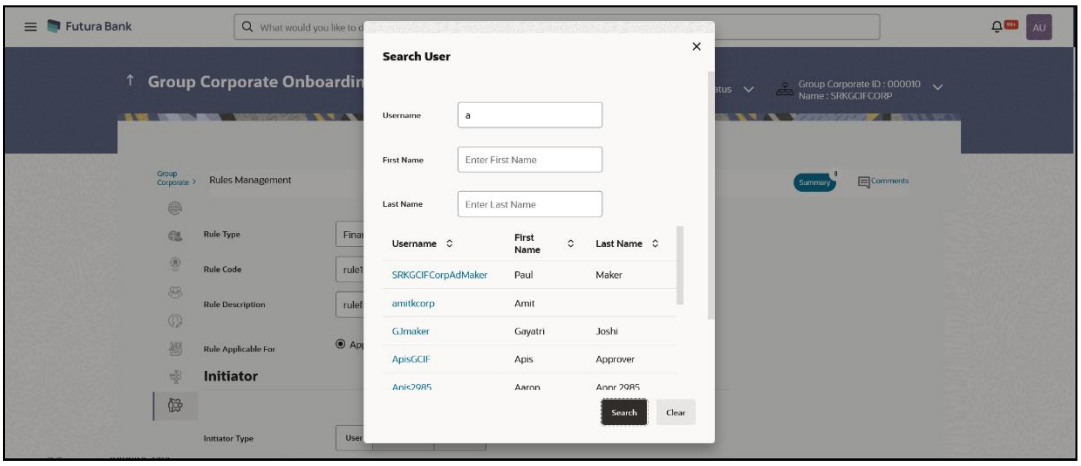
Field Name	Description
Currency	Currency type in which the financial approval rule for a corporate is defined. This field appears if you select **Financial** and Non Account Financial in the **Rule Type** field. Note: 1) Entity's base currency (maintained in system configuration) will be defaulted in the currency field. 2) User will be able to select the currency other than the default currency from the currency list.
Amount Range	
From Amount/ To Amount	Transactions allowed for the user between the amount range. This field appears if you select **Financial** and Non Account Financial in the **Rule Type** field.
Workflow Details	
Approval Required	Option to decide whether approval is required or not for the set condition. The options are: • Yes • No
Approval Type	Define the Approval workflow type. Possible value will be • Sequential • Parallel This field is enabled if **Yes** option is selected in **Approval Required** field and when workflow preference is set at **Rule Level** in Group Corporate Profiling setup.
Workflow	All workflows maintained for the party are listed here along with the defined approval level for each of them. Select one workflow within which different levels are available for approver and checker. For release, the release workflow can be selected. This field appears if you select **Yes** in the **Approval Required** field.

To create an approval rule for corporate user:

1. In the **Rule Type** field, select the appropriate transaction rule type.

2. In the **Rule Code** field, enter the code.
3. In the **Rule Description** field, enter the rule name.
4. In the **Rule Applicable For** field, specify the rule applicable for Release or Approval.
5. From the **Initiator Type** field, click appropriate user / user group and select the user/ user group or Select ‘All Users’.
6. Click icon to add appropriate user / user group. The **Search User to Copy Mapping** popup appears.

Approval Rules – Search User



Field Description

Field Name	Description
Search	
User ID	To search the user with the user ID. Partial search is allowed.
First Name	Allows to search based on first name or given name of the user.
Last Name	Allows to search based on last name/ surname of the user.
Search Results	
User ID	User ID of the user.
Full Name	Full Name of the user.

   a. From the **User Name / User Groups** list, click & select the user ID.
7. Click **Add** to add the selected user/ user group as a initiator.

8. From the **Party ID** list, click and select one or multiple Party IDs to be mapped to the selected Group Corporate ID.
9. From the **Transaction** list, select the transactions to be mapped to the rule.
    a. If you have selected **Select Specific Transactions** option, select one or multiple transactions within modules to mapped to the selected Group Corporate ID.

    Note: Click icon to search and add specific transaction from the search lookup.

10. If you have selected **Financial** option in the **Rule Type** field;
    a. From the **Accounts** list, select the appropriate accounts.
        i. If you have selected **Select Specific Accounts** option;
            1. Click the Party ID whose accounts needs to be mapped, and then select one or multiple accounts to mapped to the selected Group Corporate.

            Note: Click icon to search and add specific account from the search lookup.

    b. From the **Currency** list, select the appropriate account currency.
11. If you have selected **Financial** and **Non Account Financial** option in the **Rule Type** field;
    a. In the **Amount Range** section, enter the appropriate amount.
12. In the **Workflow Details** section, select whether approval is required for the mapped transactions.
    a. If you select **Yes** option,
        i. In the **Approval Type** field, select approval workflow type.
        ii. From the **Workflow** list, select the appropriate Workflow.
13. Click **Save** to save approval rule.
    OR
    Click **Back** to navigate back to previous screen.
    OR
    Click **Submit** to submit the steps performed so far for approval.
    OR
    Click **Retain Draft** to save the details entered as draft.
    OR
    Click **Cancel** to cancel the transaction.
14. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click on **Add Another** to Add The **Approval Rule.**
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate back to previous screen.
15. The success message of saving the created approval rule appears along with the transaction reference number and status.

Send to Modify

Approver dashboard is available for Bank administrator users whose main responsibility is of approving the transactions initiated by Bank administrator in maker role. Approver has the responsibility to ensure correctness of the maintenances as per the bank and corporate mandate, to ensure speedy and accurate processing.

When the maker sends the Group Corporate Onboarding maintenance for approval, the approver will have an option to send the maintenance back for modification.

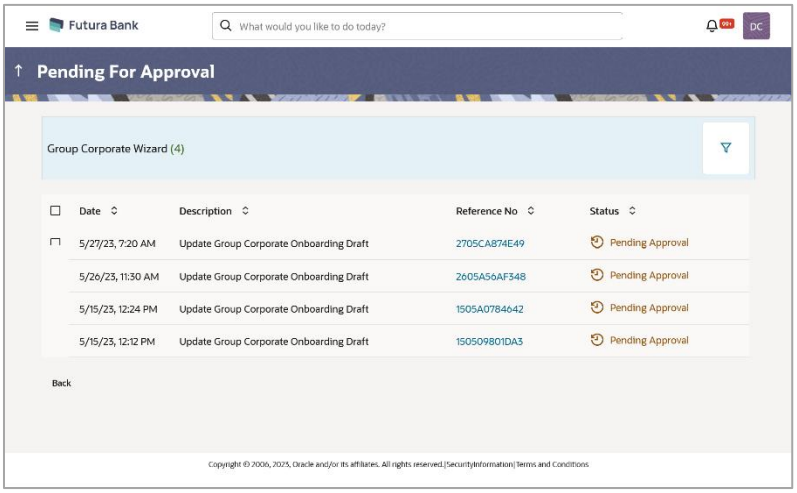
When the transaction is sent back for modification, then all the users who have access to perform modifications on Group Corporate onboarding will be able to view the maintenance in their activity log. Any of the users can pick up the transaction and make the necessary modification.

Note: During **Send to Modify**, the comments capture by approver are optional. The bank needs to handle operationally to ensure that specific comments are captured during send for modification.

1. Login to OBDX internet banking application as an approver.
2. Navigate to:

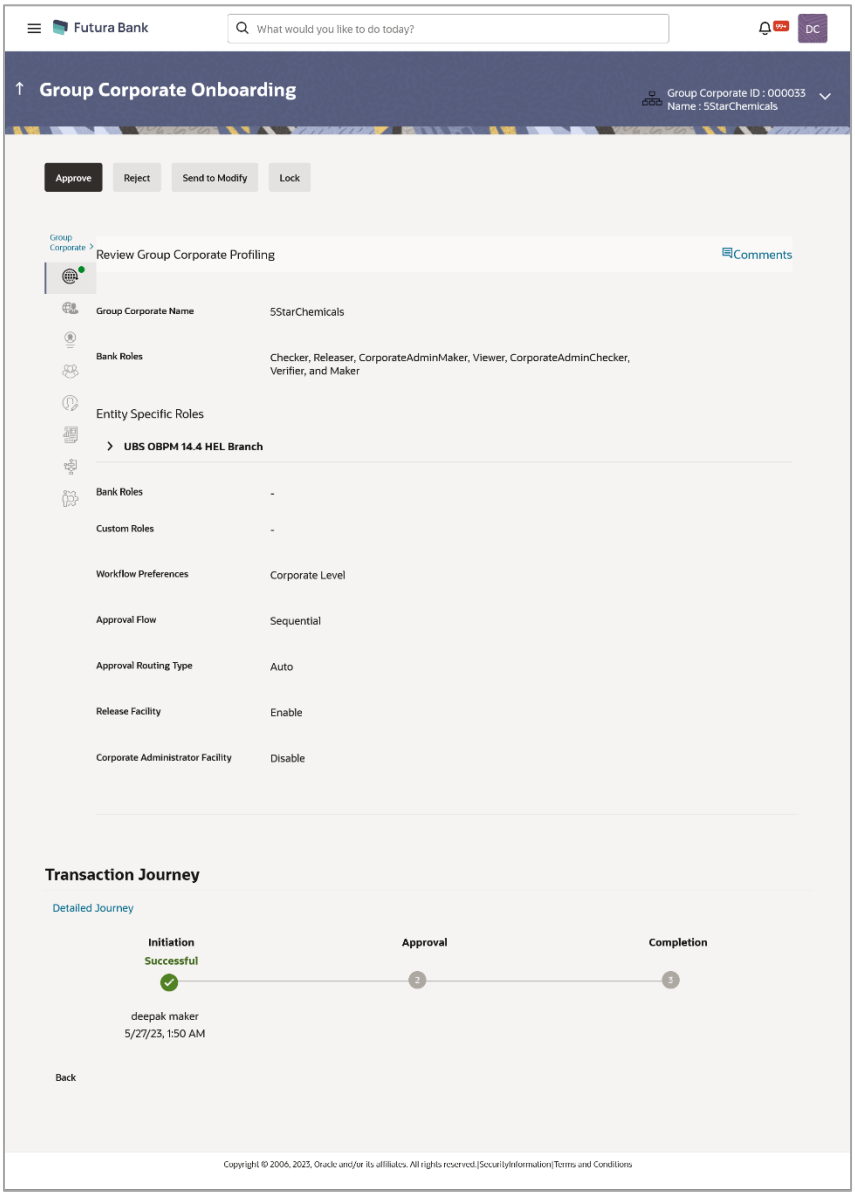
Bank Administrator Dashboard > Toggle menu > Menu > Transactions > Pending for Approval > select Group Corporate Wizard

Send to Modify - Pending for Approval screen



7. Click on the **Reference No** link adjacent to record which to be modify/ approve/reject/lock. The Group Corporate Onboarding screen appears.

Send to Modify – Group Corporate Onboarding screen



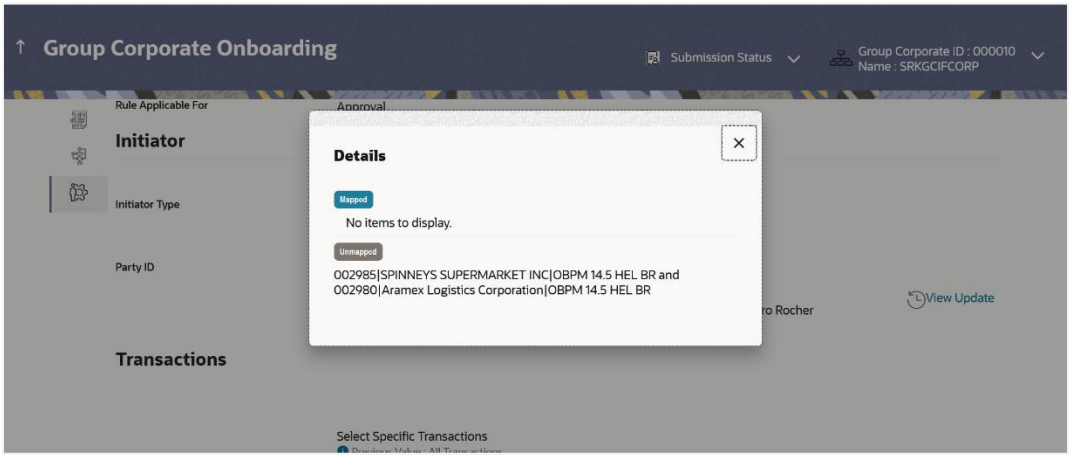
8. Click **Send to Modify** to send the Group Corporate Onboarding maintenance back to maker for modification. A popup appears.
9. Enter the comments while sending for modification to specify the reason for sending the maintenance for modification.
10. Click **Send to Modify** to save the comments and send the maintenance to maker for modification.
    OR
    Click **Cancel** to cancel the transaction.
11. Now login to OBDX internet banking application as an maker.

12. View the **Group Corporate Onboarding maintenance** in **My Initiated List** tab from the **Transactions** menu, and make the necessary modifications and send back to approver.
13. On re-login as approver, then the modified data will be highlighted for the approver to understand the changes.

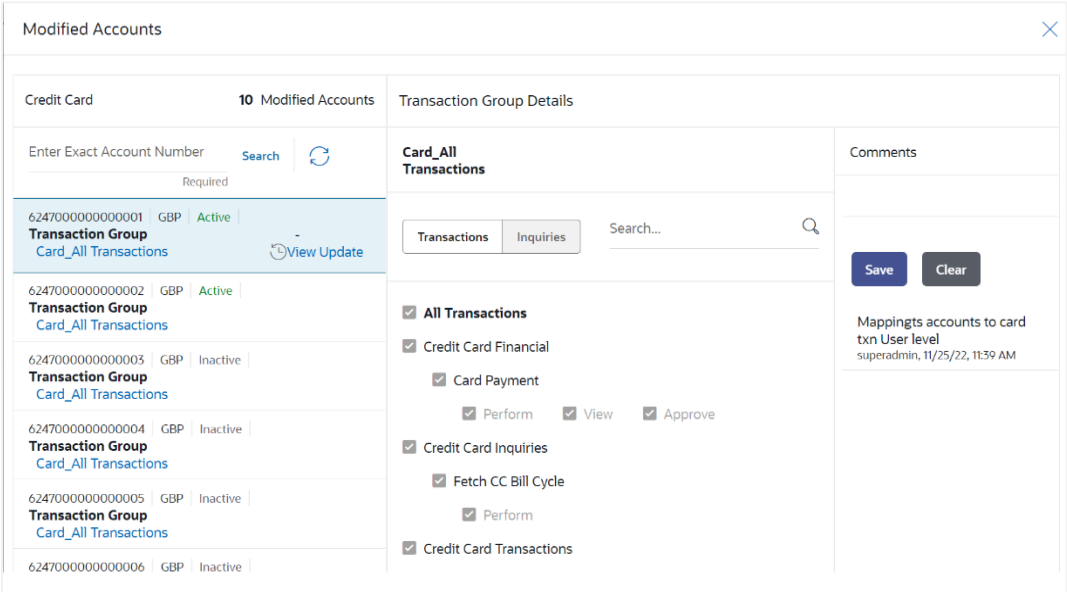
Note:
1) For all the updated values, the previous as well as new value will be shown

The modified value will be highlighted even in cases when the maker modifies any existing data and send it for approval
2) Click on the **View Update** to view the new changes in case the field has multiple values.

View Update



Modified data highlight



14. Click on highlighted data to view the modifications.
15. Verify the changes and approve the transaction.

FAQ

Step 1: Group Corporate Profiling

1. Can administrator modify Bank role before assigning to Group Corporate?

No, if the Administrator assigns a Bank role to Group Corporate, all the entitlements available in the selected roles will be assigned at Group Corporate level. Any modification required in the bank roles can be done using Role transaction mapping screen. If in future bank assigns a new transaction access in the bank role (from Role transaction mapping screen), it will automatically be given to the all the Group Corporates having that roles mapped

2. Is mapping of custom role is mandatory?

No. Administrator can select and assign the roles available at enterprise level as is, or he can create a custom role as per his requirement for the Group corporate by cloning a role available at Group Corporate level.

Admin will be able to assign a mix of bank roles and custom roles to a Group Corporate.

3. Are the Customize bank roles will be applicable across the application?

No, The Customize bank role will be available only for the Group Corporate for which it was created. Any changes done in the bank roles, from which this custom role has been created, will not have any impact on the custom created roles

4. **What is sequential and parallel type of approval flow?**

   Under Sequential approval flow, the approval can be done only in the sequence as mentioned in approval workflow. It is “Non-Sequential” type of approval flow, which does not follow any specific sequence. Any user (who is part of the approval flow) from any approval level can pick up the transaction/maintenance and approve it. This will be applicable across Group Corporate

5. **What is the approval currency?**

   Approval Currency is the preferred currency for setting up the approval rules.

6. **How can the user define Sequential or Parallel approval flow at the Corporate Level and Rule Level?**

   During Group Corporate Profiling setup, the user has an option to select the workflow preference at Corporate Level or Rule Level. If Corporate Level is specified, then the approval flow (Sequential/Parallel/No Approval) can be captured on the same screen. If Rule Level is selected, then the approval flow (Sequential/Parallel) must be specified during rule creation.

Step 2: Party Account Access

5. **Is it necessary to setup Party Account Access Management before setting up User Account Access for Group Corporate?**

   Yes. For the Group Corporate, the party account access setup must be done before the user level mapping of accounts and transactions

6. **What is the significance of Transactions or Inquiry Group?**

   Transaction groups are for the purpose of grouping transactions and maintaining access in Account Access screens.

   There will be one factory shipped Transaction group for each module, which will have all transactions and inquiries grouped together. Factory shipped user group cannot be deleted or modified.

   A new group can also be created by cloning/copying an existing transaction group. Deletion of custom transaction group will be allowed.

   Transaction groups of one Group Corporate will be available for selection only for that Group Corporate

7. **Can we setup Party Account Access for multiple corporate parties associated with Group Corporate in single flow?**

   Yes, All the party ID mapped under Group Corporate will be listed in the dropdown. Admin can select one party at a time and setup the party account access for the same .Once he is done he can follow the same flow by selecting another party for Account maintenance before final submission.

OR

He can save the application in draft for further modification.

8. What is the significance of Auto and Manual option in 'Map Accounts'?

This feature allows the administrator to configure access policies for accounts and associated transactions, which may get added subsequently in the future.

Auto: Gives access to the newly added accounts and transactions of the party as soon as the account is opened. This option can be selected whenever bank administrator wishes to provide access by default

Manual: Denies the newly added accounts and transactions by default. This is to ensure that access to accounts and transactions is provided only upon receiving specific instructions from corporates

9. Will Party Account Access – Deletion for a party (Own/Linked) lead to automatic deletion of User Account Access?

Yes. Deletion of account access for a party will lead to automatic deletion of access for the users of that party.

Step 3: User Onboarding

1. Who can create / update the user at Group Corporate level?

System administrator and bank administrator can create or edit the users.

2. Does the application allows admin to create new user by cloning the exiting one?

Yes. An option to create a new user from by copying an existing user is provided.

If 'Copy' is selected, admin will be able to select an already created user (user created under the same Group Corporate) and screen will be displayed the copied data for all the sections except Personal and Contact information. Admin will be require to fill Personal and Contact information and he can make the changes in the copied data as well.

3. Can one assign multiple Application roles to a user?

Yes, multiple Application roles can be assigned to the user. All the Roles (both Enterprise and Customer) mapped at the Group Corporate level will be available for selection while setting up the user management.

4. What is the significance of primary and Accessible parties?

Corporate users at Group Corporate level will have one primary party and multiple assessable parties for each entity. Show primary party selected on the top will by default as selected under Primary Party for that Entity.

Step 4: User Group Maintenance

1. Is the user selection for user group maintenance is depends on the parent party?

No, user selection is not depend upon the parent corporate party. Application will list down the entire user associated with group corporate for user group creation irrespective of parent party.

2. Can a user be the part of multiple user groups created under a Group Corporate?

Yes, same user can be part of multiple user groups under group corporate. Whereas, User Group would be allowed to create even without adding a single user

3. Can I delete an existing user group?

No, user groups cannot be deleted but can be edited. Administrator can add new users and remove existing users of the user group.

Step 5: User Account Access

1. **If user is associated with one parent corporate party and multiple accessible parties, then will he be allowed to setup account access for the corporate parties in single flow?**

   Yes, All the party ID mapped under Group Corporate and associated with corporate user will be listed in the dropdown. Admin can select one party at a time and setup the user account access for the same .Once he is done he can follow the same flow by selecting another party for user Account maintenance before final submission.

   OR

   He can save the application in draft for further modification.

2. **Will Party Account Access – Deletion for a party lead to automatic deletion of User Account Access?**

   Yes, deletion of account access for a party will lead to automatic deletion of access for the users of that party.

3. **If I remove access of account(s) and transaction(s) for a party, will it lead to automatic access removal for the users of that party?**

   Yes, access removal at party level for an account and/or transaction will automatically remove access at user level of the selected party.

4. **Have mapped/edited/deleted user account access for a party but it is not reflecting in the system even after a successful maintenance save message?**

   There is a possibility that the maintenance is saved but the status is ‘Pending Approval’. For the maintenance, if there is an approval required then the changes will reflect only once the approver(s) approve the submitted request. If the setup does not require an approval workflow or is self / auto approved, then the same will reflect immediately.

Step 6: User Report Mapping

1. **What is the significance of user report mapping?**

   The user report mapping maintenance allows the Bank Administrators to map the report or set of reports to a specific corporate user. The corporate users can generate and view the reports to which they have an access.

2. **Is the user selection for user report mapping maintenance is depends on the parent party?**

   No, user selection is not depend upon the parent corporate party. Application will list down the entire user associated with group corporate for user report mapping irrespective of parent party.

Step 7: Workflow Management

1. **Is the user selection for workflow maintenance is depends on the parent party?**

   No, user selection is not depend upon the parent corporate party. Application will list down the entire user associated with group corporate for workflow maintenance irrespective of parent party.

2. **What is approval workflow maintenance?**

   Approval workflows are created to support requirements where multiple levels of approval are required in a specific sequence for a transaction/maintenance. Each workflow can be configured to have up to five levels of approval with a specific user or a user group configured at each level.

3. **How many approval levels can I set up in the system?**

   Administrator can set up minimum one and maximum five levels of approvals as a part of approval workflow.

4. **Can I get the list of users associated with a group from workflow management screen?**

   Yes, list of the users associated with a group can be viewed using workflow management screen.

Step 8: Approval Rules

1. **Is the user selection for workflow maintenance is depends on the parent party?**

   No, user selection is not depend upon the parent corporate party. Application will list down the entire user associated with group corporate for approval -rules maintenance irrespective of parent party.

2. **How many approval levels can I set up in the system?**

   Administrator can set up minimum one and maximum five levels of approvals as a part of approval workflow. Whereas, maximum levels of approvals that the user can set is configurable as Day0.

10. **Explain by examples how the rules are resolved during auto and manual approval routing?**

    If the Day 0 configuration is yes (i.e., weightage needs to be checked), then the rules will be evaluated irrespective of the currency. However, the final rule which is resolved will be as per the calculated weightage.

ORACLE

If the Day 0 configuration is no (i.e., weightage need not be checked), then the rules will be evaluated irrespective of the currency, and all the rules falling within the amount range (post currency conversion) will be resolved. For Manual Routing, whichever rule the maker picks up will be the resolved rule. For Auto Routing, the nearest 'max' value logic will be checked and the rule with nearest max slab will be evaluated. However, if two rules have the same nearest 'max' slab, then whichever approver picks the transaction first, that rule will be the final resolved rule.

Some use cases are listed below for better understanding:

Use Case 1: Rule CCY = TXN CCY

Maintenance	System Behavior
Entity Base CCY – AED Approval Type – Auto Routing Rules maintained are as follows: Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – BHD, Amount Range 5k to 10k The customer is initiating a transaction in BHD 9K (equivalent to USD 23.8k, QAR 86.9k) *Considering all other rule criteria are matching	Applicable Rules*: Day 0 – when weightage check is enabled Rule 3 - CCY – BHD, Amount Range 5k to 10k Reason – System will evaluate all the rules irrespective of any currency. The rules (Rule 1, Rule 2 and Rule 3) falling within the transaction range will be resolved, however as per the weightage logic, the rule maintained in TXN CCY will have higher weightage. Hence only Rule 3 will be resolved Day 0 – when weightage check is disabled Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – BHD, Amount Range 5k to 10k Reason – System will evaluate all the rules irrespective of any currency without checking any rule weightage Note: Out of the box, the weightage check will always be enabled for auto routing.

Use Case 2: Rule CCY = Entity Base CCY

Maintenance	System Behavior
Entity Base CCY – AED Approval Type – Auto Routing Rules maintained are as follows: Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – AED, Amount Range 50k to 100k	Applicable Rules*: Day 0 – when weightage check is enabled Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – AED, Amount Range 50k to 100k

The customer is initiating a transaction in BHD 10K (equivalent to USD 26.5k, AED 97.5k, QAR 96.5k) *Considering all other rule criteria are matching	Reason – The system will check if any rule is available in the TXN CCY as per weightage logic. If the TXN CCY rule is not available, all the other rules irrespective of any CCY will be applicable provided it matches the amount slab Day 0 – when weightage check is disabled Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – AED, Amount Range 50k to 100k Reason – System will evaluate all the rules irrespective of any currency without checking any rule weightage Note: Out of the box, the weightage check will always be enabled for auto routing.

Use Case 3: Rule CCY = Multiple TXN CCY rules

Maintenance	System Behavior
Entity Base CCY – AED Approval Type – Auto RoutingRules maintained are as follows: Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – BHD, Amount Range 5k to 10k Rule 4 - CCY – BHD, Amount Range 9k to 10k Rule 5 - CCY – BHD, Amount Range 10k to 50k Rule 6 - CCY – AED, Amount Range 50k to 100k The customer is initiating a transaction in BHD 10K (equivalent to USD 26.5k, AED 97.5k, QAR 96.5k) *Considering all other rule criteria are matching	Applicable Rules*: Day 0 – when weightage check is enabled Rule 3 - CCY – BHD, Amount Range 5k to 10k Rule 4 - CCY – BHD, Amount Range 9k to 10k Reason – System will evaluate all the rules irrespective of any currency, however as per the weightage and 'to/max' amount logic, the rule maintained in TXN CCY will have higher weightage. Hence Rule 3 and Rule 4 will be resolved. Based on the users approving at each level, exact rule will be determined Day 0 – when weightage check is disabled Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – BHD, Amount Range 5k to 10k Rule 4 - CCY – BHD, Amount Range 9k to 10k Rule 5 - CCY – BHD, Amount Range 10k to 50k Rule 6 - CCY – AED, Amount Range 50k to 100k Reason – System will evaluate all the rules irrespective of any currency without checking any rule weightage Note: Out of the box, the weightage check will always be enabled for auto routing.

Use Case 4: Rule CCY = TXN CCY (Flexi Routing)

Maintenance	System Behavior
Entity Base CCY – AED Approval Type – Flexi Routing Rules maintained are as follows: Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – BHD, Amount Range 5k to 10k Rule 4 - CCY – BHD, Amount Range 9k to 10k Rule 5 - CCY – BHD, Amount Range 10k to 20k Rule 6 - CCY – AED, Amount Range 50k to 100k The customer is initiating a transaction in BHD 9K (equivalent to USD 23.8k, AED 87.6k, QAR 86.9k) *Considering all other rule criteria are matching	Applicable Rules*: Day 0 – when weightage check is enabled Rule 3 - CCY – BHD, Amount Range 5k to 10k Rule 4 - CCY – BHD, Amount Range 9k to 10k Reason – System will evaluate all the rules irrespective of any currency, however as per the weightage and 'to/max' amount logic, the rule maintained in TXN CCY will have higher weightage Day 0 – when weightage check is disabled Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – BHD, Amount Range 5k to 10k Rule 4 - CCY – BHD, Amount Range 9k to 10k Rule 5 - CCY – BHD, Amount Range 10k to 20k Rule 6 - CCY – AED, Amount Range 50k to 100k Reason – System will evaluate all the rules irrespective of any currency. Maker will be expected to select one rule and route for approval.

Use Case 5: Sequential/Non-Sequential Rules (Flexi Routing)

Maintenance	System Behavior
Entity Base CCY – AED Approval Type – Flexi Routing Rules maintained are as follows: Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – BHD, Amount Range 5k to 10k (Sequential) Rule 4 - CCY – BHD, Amount Range 9k to 10k (Non-Sequential) The customer is initiating a transaction in BHD 9K (equivalent to USD 23.8k, QAR 86.9K) *Considering all other rule criteria are matching	Applicable Rules*: Day 0 – when weightage check is enabled Rule 3 - CCY – BHD, Amount Range 5k to 10k (Sequential) Reason – System will evaluate all the rules irrespective of any currency, however as per the weightage and 'to/max' amount logic, the rule maintained in TXN CCY will have higher weightage. In this case based on the Day0 configuration, the default behavior is 'Sequential' rule which needs to be given precedence. However, bank can change this configuration to 'Non-sequential' rule to be given precedence Day 0 – when weightage check is disabled Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k

	Rule 3 - CCY – BHD, Amount Range 5k to 10k Rule 4 - CCY – BHD, Amount Range 9k to 10k Reason – System will evaluate all the rules irrespective of any currency. Maker will be expected to select one rule and route for approval.

Use Case 6: Sequential/Non-Sequential Rules (Auto Routing)

Maintenance	System Behavior
Entity Base CCY – AED Approval Type – Auto Routing Rules maintained are as follows: Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – BHD, Amount Range 5k to 10k (Sequential) Rule 4 - CCY – BHD, Amount Range 9k to 10k (Non-Sequential) The customer is initiating a transaction in BHD 9K (equivalent to USD 23.8k) *Considering all other rule criteria are matching	Applicable Rules*: Day 0 – when weightage check is enabled Rule 3 - CCY – BHD, Amount Range 5k to 10k (Sequential) In case of auto routing, based on the Day0 configuration, the default behavior is 'Sequential' rule which needs to be given precedence. However, bank can change this configuration to 'Non-sequential' rule to be given precedence Day 0 – when weightage check is disabled Rule 1 - CCY – USD, Amount Range 5k to 25k Rule 2 - CCY – QAR, Amount Range 50k to 100k Rule 3 - CCY – BHD, Amount Range 5k to 10k Rule 4 - CCY – BHD, Amount Range 9k to 10k Reason – System will evaluate all the rules irrespective of any currency. Maker will be expected to select one rule and route for approval.

Use Case 7: Rule Weightage Logic

Entity Base CCY – **AED**
Rules maintained are as follows:

Rules	Accounts	Transactions	CCY	Amount Slab	Approval Flow
Rule 1	10000909 10000908 10000907	All Financial Transactions <International Fund Transfer is a part of Payment Transaction Group>	USD	5k to 25k	Group A > Group B > Group C

Rule 2	All Accounts	International Fund Transfer	AED	50k to 100k	Group A > Group D > Group E
Rule 3	All Accounts	International Fund Transfer	BHD	5k to 10k	Group A > Group C > User X
Rule 4	10000908 10000907	International Fund Transfer, Multiple Payment Transactions	BHD	9k to 10k	User P > User Q

The customer is initiating an **International Fund Transfer** from account **10000907** of **BHD** 9K (equivalent to USD 23.8k, AED 87.6k)

Applicable Rules:

Auto Routing (when weightage check is enabled) -

Rule 4 - CCY – **BHD,** Amount Range 9k to 10k

Reason – System will first check if the matching rule is available in TXN CCY (BHD). There are 2 rules available in BHD, Rule 3 and Rule 4. However, in auto routing only Rule 4 will be resolved as specific values are maintained for account and transactions as compared to Rule 3.

Flexi Routing (when weightage check is disabled) -
Rule 1- CCY – **USD**, Amount Range 5k to 25k
Rule 2- CCY – **AED**, Amount Range 50k to 100k
Rule 3 - CCY – **BHD**, Amount Range 5k to 10k
Rule 4 - CCY – **BHD**, Amount Range 9k to 10k

Reason – System will evaluate all the rules irrespective of any currency. As all the rules fall within the amount range, hence all the rules will be displayed to the user for selection.

16. Party Migration

Using this feature a party can be moved from one Group Corporate to another Group Corporate. System displays a screen to enter the party information (party ID or party name) and search party for which the movement of party is to be done. Party migration can be updated to an existing or new Group Corporate.

Before movement, a simulation needs to be generated to show the conflicts/impacted areas due to Party migration. The simulation will be generated module wise to view impact of party migration. The user can view the current generated simulations as well as the historical simulations generated for the movement of selected Party ID.

The administrator must manually take corrective actions on the conflicting impacted areas, post which only the party migration can be initiated.

Note: After rectification of all conflicted impacts, the simulation needs to be re-generated to validate for any remaining conflicts

The impact of Party movement:

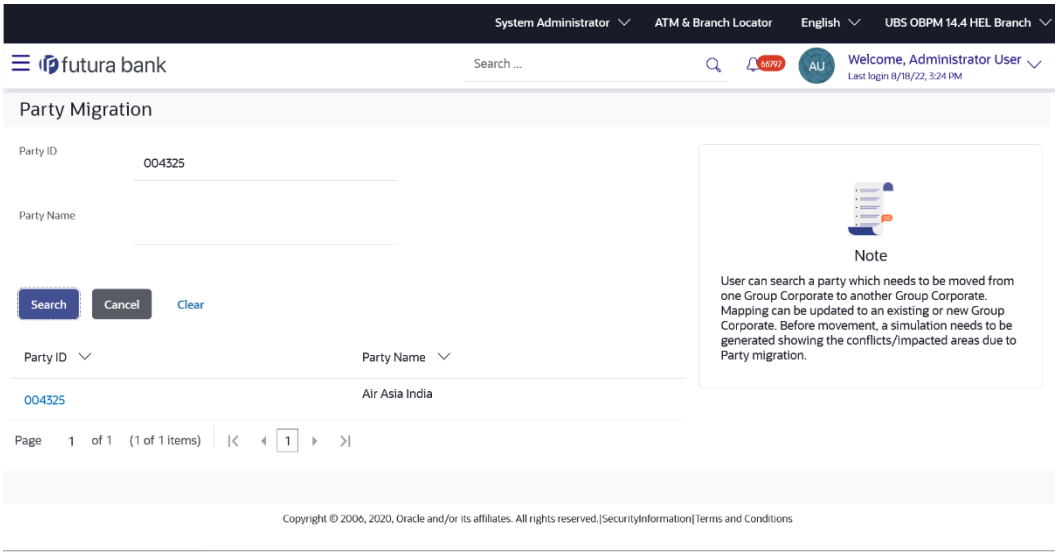
- If mapping (Party Migration) is done to an existing Group Corporate, then the common roles and touch points between the new Group Corporate and user being moved will be assigned to the respective user
- If mapping (Party Migration) is done to new Group Corporate, then a default role will be assigned to the user and touch points common to default role and respective user will be mapped to that user
- User will be able to access the reports mapped to the user at Party level even after moving the Party under new Group Corporate
- The user's personal and contact information along with limits will be retained during movement to the new Group Corporate
- Moved Party will not be available under the old Group corporate and any mapping of the moved Party with the users of old Group Corporate will get deleted
- Any approval rule created exclusively for the accounts of moved Party will not be automatically moved along with the Party
- The users moving to new Group Corporate along with the Party will not be able to view the details of transactions/maintenances (happened in the other Party s of previous Group Corporate) where they have acted as either 'maker or approver'.
- The users moving to new Group Corporate along with the Party will be able to view the details of transactions/maintenances (happened in the Party before movement) where they have acted as either 'maker or approver'. They will be able to view this data through their respective activity logs
- Also, the users who are part (either maker or approver) of any transaction/maintenance in the Party before movement, and are not moving with the Party , will not be able to view that data in their respective activity logs
- If the user being moved has a User Level Alert Subscription, then the Alert Subscription Configuration will be retained for the Party being moved but will be dropped for other Party s

Once the admin user simulates the party movement and all the conflicts are resolved, the user can migrate the party to new group corporate. On submission, the maintenance is sent for an approval if configured. Once the maintenance is authorized, the party will get mapped to the new Group corporate. Post party migration, the user can search the Party based upon Party ID or Party Name and view details of the movement. Details related to all the impacted areas will be displayed. This data will be available module wise which can be viewed as well as downloaded in PDF format. The migration information of the historic movements can also be viewed if in future the same party needs to be migrated again.

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Corporate Onboarding > Party Migration
OR
System/ Bank Administrator Dashboard> Corporate Onboarding widget > Party Migration

Party Migration – Party Search (Party ID/Party Name)



Field Description

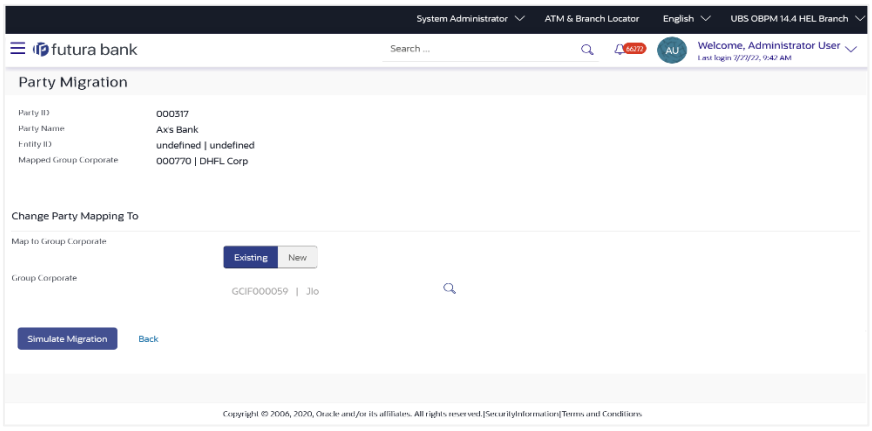
Field Name	Description
Search	
Party ID	Search by party ID for which the party migration to be done.
Party Name	Search by party name of a party for which the party migration to be done.
Search Result	

Field Name	Description
Party ID	Party ID for which the party migration to be done.
Party Name	Party Name of a party for which the party migration to be done.
Status	Displays the status of the searched party. It could be: • Simulation in Conflict • Migration Success

To search party for party migration and generate the stimulation report:

1. In the **Party ID** field, enter the party ID whose party migration to be done.
   OR
   In the **Party Name** field, enter the name of the party whose party migration to be done.
2. Click **Search**. The system displays the matching party records. The records have parties listed with both **Party ID** and **Party Name** information. User can select the record by clicking on the **Party ID** from the list.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction.
3. Click on the **Party ID** link to view the existing Group Corporate ID and Name to which the Party is currently mapped.

Party Migration – Map to Existing/ New Group Corporate



Field Description

Field Name	Description
Party ID	Displays the Party ID for which the party migration is to be done.
Party Name	Displays the Name of the party for which the party migration to be done.
Entity ID	Displays the Entity ID of the Corporate Party. **Note:** Party Migration is allowed within same entity.
Mapped Group Corporate	Displays the existing Group Corporate ID to which party is mapped.
Change Party Mapping To	
Map to Group Corporate	Specify if new mapping for Party is to an existing Group Corporate or to a new Group corporate.
Group Corporate	Group Corporate ID for which party migration is to be done.
Search Group Corporate	
This popup appears, if user wishes to move Party to existing Group Corporate.	
Group Corporate ID	Search by existing Group Corporate ID to which the Party is being moved.
Group Corporate Name	Search by existing Group Corporate Name to which the Party is being moved.
Search Result	
Group Corporate ID	Existing Group Corporate ID to which the Party is being moved.
Group Corporate Name	Existing Group Corporate Name to which the Party is being moved.

4. In **Change Party Mapping To** section,
   a. In **the Map to Group Corporate** field, select the desired option for new mapping for Party whether it is from an existing Group Corporate or to a new Group corporate.
   b. If **Existing** option is selected in the **Map to Group Corporate** field,
      i. Click icon against the **Group Corporate** field, the **Search Group Corporate** popup window appears.

1. Click and enter the Group Corporate ID in the **Group Corporate ID** field to which the Party is being moved.
   OR
   In the **Group Corporate Name** field, enter the existing name of the Group Corporate to which the Party is being moved.
2. Click **Search**. The existing Group Corporate appears based on search criteria.
   OR
   Click **Reset** to reset the details.

c. If **New** option is selected in the **Map to Group Corporate** field,

i. In the **Group Corporate** field, enter the new Group Corporate to which the Party is being moved.

ii. Click **Check Availability** to check the uniqueness of the user ID. If the Group Corporate is already used, then enter a unique valid Group Corporate name.

5. Click **Simulate Migration** to generate reports module wise showing module wise impact of party migration . User can also view the report generation status.
   The **Warning** popup appears to restrict the channel access to the party while the simulation is being generated so that no further changes to the party will be allowed.

Simulate Migration Warning popup

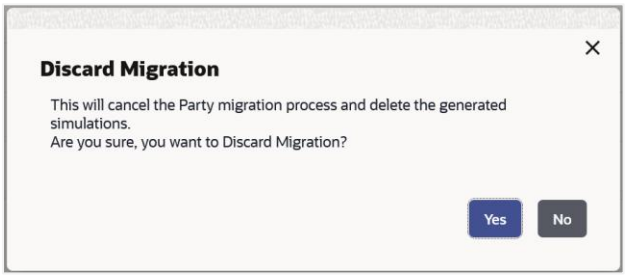
a. Click **Proceed** to continue the process.
   In **Simulation** section list of total reports generated after stimulation gets displayed.
   OR
   Click **Cancel** to cancel the transaction.

b. Click ▶ icon to expand and view the details of reports module wise.

c. Click on the **Download** link against the respective module to download the stimulation migration report.

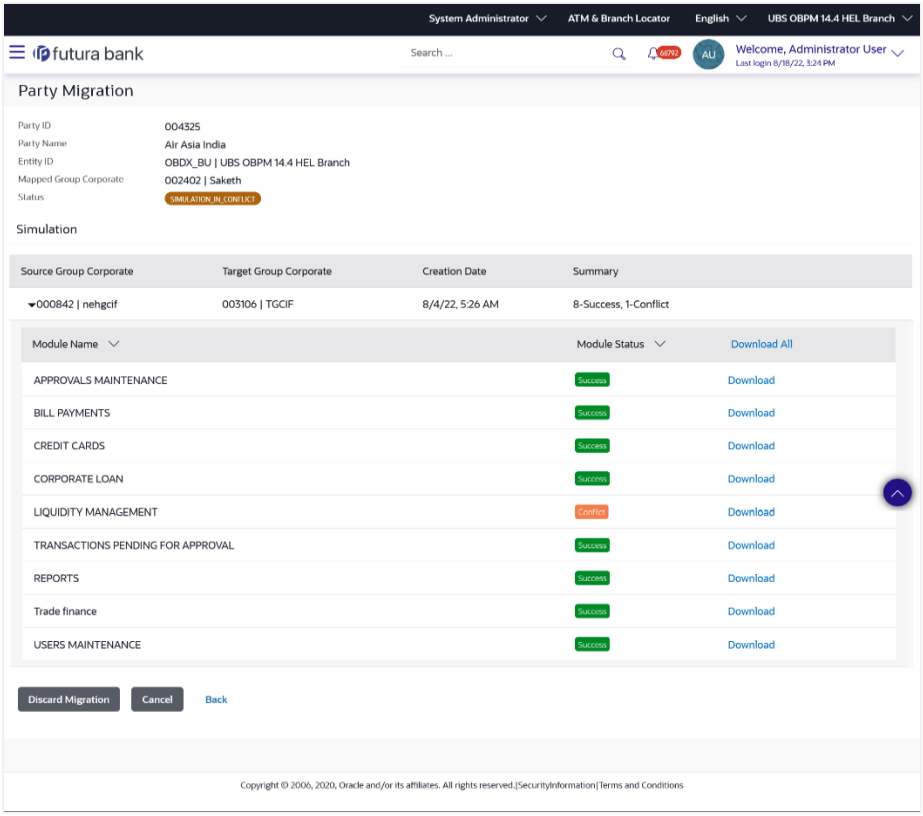
OR
Click **Discard Migration** to revert the party migration changes. It removes all the simulation reports generated from the system for the party being moved.

Discard Migration popup



OR
Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate back to the previous screen.

Simulate Migration



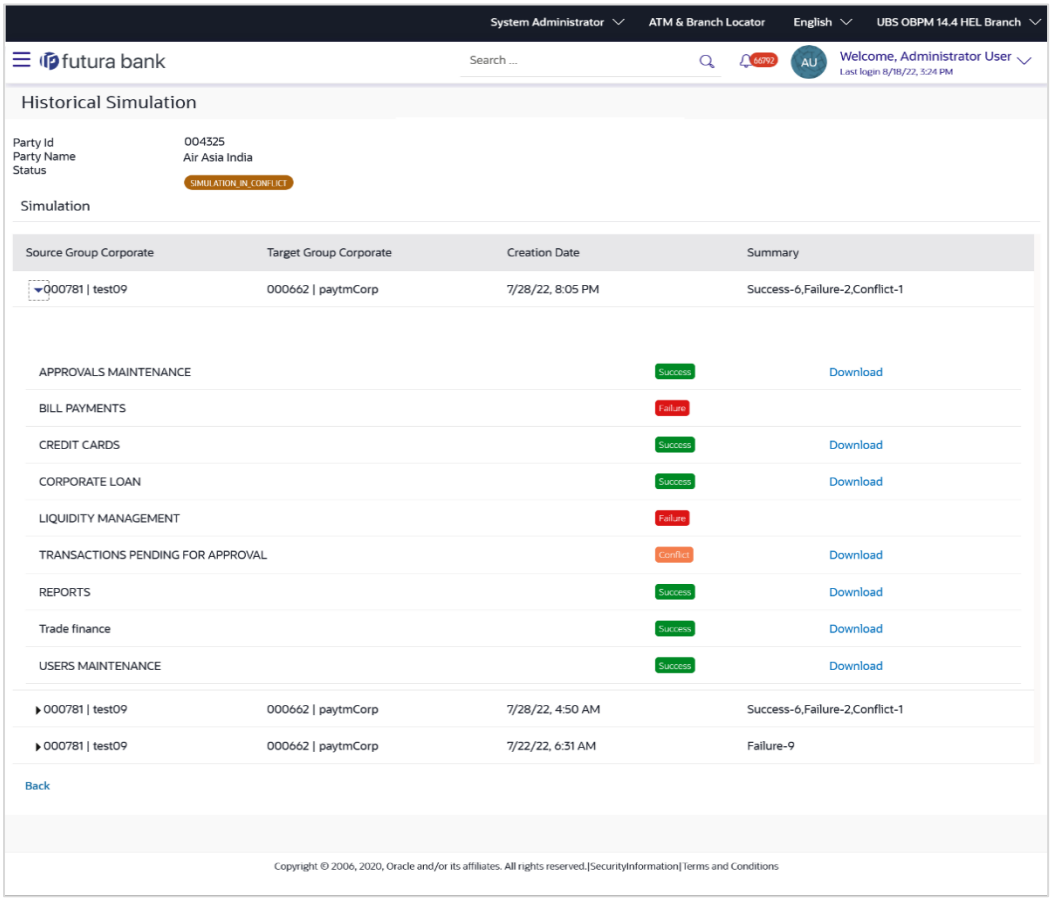
Field Description

Field Name	Description
Party ID	Displays the Party ID for which the party migration to be done.

Field Name	Description
Party Name	Displays the Party Name of a party for which the party migration to be done.
Entity ID	Displays the Entity ID of the Corporate Party. **Note:** Party migration is allowed within same entity.
Mapped Group Corporate	Displays the existing Group Corporate ID to which party is mapped.
Status	Displays the stimulation status.
Simulation	
Following fields appears after the stimulation report is generated module wise for the party is being migrated.	
Party ID	Displays the Party ID for which the party migration to be done.
Party Name	Displays the Party Name of a party for which the party migration to be done.
Source Group Corporate	Displays the existing Group Corporate ID to which party is mapped.
Target Group Corporate	Specify new Group Corporate to which the Party is being migrated.
Creation Date	The date and time of stimulation report generated.
Summary	Displays the summary of total stimulation report generated along with its status and count. The options are: • Success • Failed • Conflict • Pending
Module Name	Name of the module whose stimulation reports are generated before party migration.

Field Name	Description
Module Status	The simulation generation status can also be viewed. The options are: • Success: Party impact present with no conflict • Failure: Simulation fails due to technical error • Conflict: Simulation comprises of atleast one conflict • Pending: Awaiting for response
Download	Click on the **Download** link to download the respective simulation in PDF format. **Note:** Click on the D**ownload All** link to download all the modules reports.

Historical Simulation



Field Description

Field Name	Description
Historical Simulation	
This section displays the all the previous list of stimulation reports. Following fields appears after the stimulation report is regenerated module wise for the party is being migrated. **Note:** This section is displayed only if the stimulation report is generated for the same party multiple times to resolved the Failure /Conflict type of report.	
Party ID	Displays the Party ID for which the party migration to be done.
Party Name	Displays the Party Name of a party for which the party migration to be done.
Source Group Corporate	Displays the existing Group Corporate ID to which party was mapped.
Target Group Corporate	Displays the new Group Corporate to which the Party is migrated.
Creation Date	The date and time of stimulation report generated.
Summary	Displays the summary of total stimulation report generated along with its status and count. The options are: • Success • Failed • Conflict • Pending

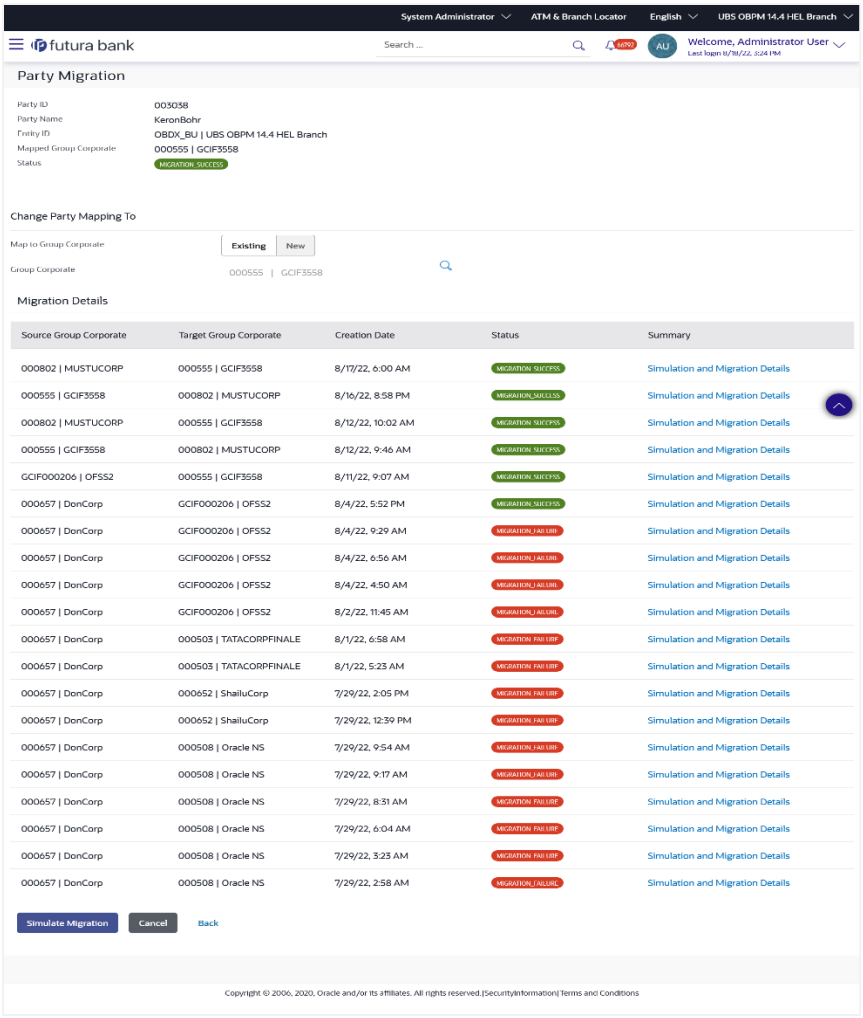
Click **Historical Migration** to view all the previous list of stimulation reports module wise.
OR
Click **Migrate Party** to initiate the request to party migration between group corporates. The **Confirmation** popup window appears.

a. Click **No** to cancel the process.
   OR
   Click **Yes** to proceed the party migration. The success message of request initiation for party migration.

   i. Click on the **Party Migration** link to view the status of the migration. System redirect to the **Party Migration** screen.

1. In the **Party ID** field, enter the party ID whose party migration is done.
   OR
   In the **Party Name** field, enter the name of the party whose party migration is done.
2. Click **Search**. The system displays the party details along with migration history details.

Post Party Migration Details



Field Description

Field Name	Description
Migration Details	This section is displayed post party migration.

Field Name	Description
Source Group Corporate	Displays the source Group Corporate ID to which party was mapped.
Target Group Corporate	Displays the new Group Corporate to which the Party is migrated.
Creation Date	Displays the date and time of party migration is executed.
Status	Displays the status of the migration.
Summary	Click on the **Simulation and Migration Details** link to view the summary of total stimulation report generated along with its status and count while migrating.

Sample Migration reports: LM Pre Migration, LM Post Migration

17. Origination Workflow Configuration

Banks across different geographies can have varied requirements with regards to sequence of steps in originations for different products.

Workflow configuration is an administrative maintenance using which the bank administrator can define the sequence of the sections in application form for each of the products as well as for the bundle application. In addition to defining the sequence in which each section should flow in an application form, the administrator can also use this feature to define which Online KYC mode is to be enabled for the prospect applicants applying for any product that belongs to a specific product category. The administrator can also wish to disable Online KYC for any product category, as required.

There will be a default workflow defined in the system as part of Day0 definition for each of the product along with identified set of steps.

You can create and maintain the priority to be assigned to each product category that can be part of a bundled application. This will dictate the sequence of steps within the bundled application form.

The bank administrator will have an option to view the default workflow for each of the products. If the sequence defined for a product does not suit the bank requirements, the administrator can opt to create a custom workflow by re-arranging the steps.

The bank administrator also will have a choice to decide on the workflow to be applied for products i.e. default / custom.

Prerequisites

- Transaction access is provided to Bank Administrator
- Default Workflow with set of steps applicable for each product category is defined in the system

Features supported in application

Workflow configuration allows Bank Administrator to:

- **Single Product Application**
  - View Default Workflow
  - View Custom Workflow
  - Edit Custom Workflow
- **Bundle Application**
  - View Default Workflow
  - View Custom Workflow
  - Edit Custom Workflow

Note:

This functionality is available for Retail as well as Small and medium Business Origination workflows.

For retail originations, joint account applications workflow configuration is allowed for supported products.

The Disbursement & Repayment step in Insta Personal Loan Applications (Generic and US Region) cannot be removed from the application form workflow as it is mandatory for the processing of insta loans.

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Others > Origination Workflow Configuration

17.1 View Workflow for a Single Product Application

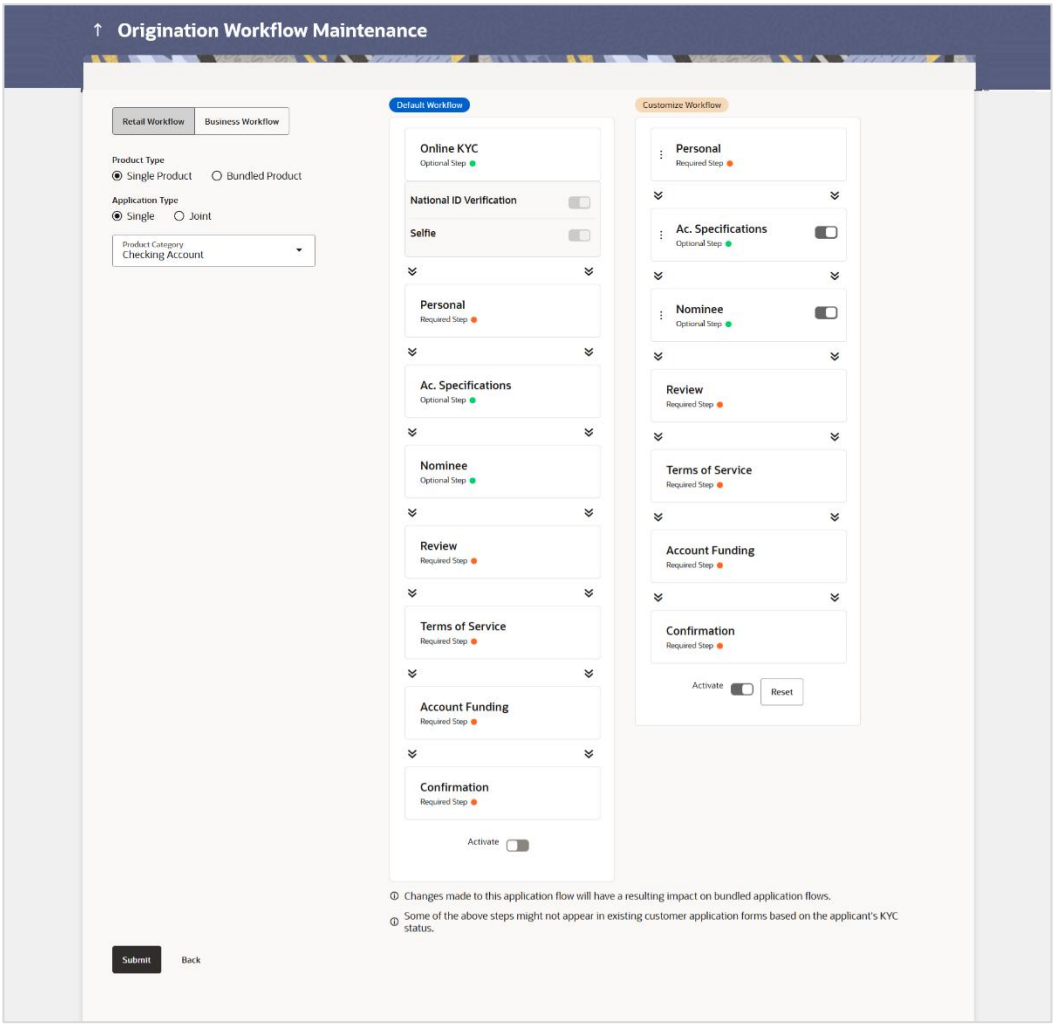
The Bank Administrator can view the retail or business workflow defined for a single product application. Both the default and the custom workflow will be visible on the landing screen side by side.

Origination Workflow Configuration

1. On the landing page, the user needs to select Workflow Type, Product Type, Application Type (if applicable) and Product Category.

   On selecting values for these fields, both the default and custom workflows for the selected Product Category and other selected parameters, appears on the screen.

Origination Workflow Configuration



Field Description

Field Name	Description
Workflow type	Workflows can be configured for Retail as well as Business products. Select the desired option. The options are: • Retail Workflow • Business Workflow

Field Name	Description
Product Type	Select the desired product application for which the workflow needs to be viewed or custom workflow is to be defined. The options are: • Single Product Application • Bundle Application
Application type	Select whether this workflow is for a single or a joint account application. This option is available for Retail Savings and Retail Checking Accounts only.
Product Category	Select the product category for which the workflow needs to be viewed or configured. The list will be populated based on the Day 0 configurations done in the application. The options available for Retail are: • Savings Account • Checking Account • Term Deposits • Credit Card • Auto Loan • Personal Loan • Home Loan • Education Loan The options available for Business are: • Savings Account • Checking Account • Term Loan • Working Capital Loan This field appears only if the **Single Product Application** tab is selected in the **Product Type** field.
Default Workflow	On the screen, the user can see a sequence of steps that will be followed by default for the given product and application type.
Custom Workflow	Adjacent to the default workflow, the user can see a custom workflow. The user can change the sequence of steps as described in upcoming sections.

Field Name	Description
Activate	An activate button is present at the bottom of both the default and custom workflows. User can select to activate one of the workflows.
Reset	This option is provided against the custom workflow. The administrator can select this option if they wish to edit the custom workflow.

2. Select the **Activate** option under either the Default or the Custom workflows to activate that workflow.

   OR

   Click the **Reset** option under the Custom Workflow to edit the custom workflow. OR
   Click **Back** to navigate to the previous screen.

17.2 Single Product Application

Using this option, Bank administrator can view the sequence in which the origination steps will be presented as a part of the default workflow to the end customer when an application is initiated for the product available under the selected product category.

Administrator can further define the custom workflow for each product category if required.

17.2.1 Edit Custom Workflow

Using this option, the bank administrator can choose to edit the custom application workflow, if required, for the specific product category. The administrator can simply drag and drop the steps to change the sequence. Additionally, the administrator can also choose to enable/disable Online KYC for product applications belonging to that product category. If enabling Online KYC, the administrator can specify which mode of Online KYC to enable. It is to be noted, that the sequence of certain steps, such as Review, Terms of Service and Confirm cannot be changed.

The administrator can even view and compare the custom workflow with the default workflow set for the selected product category and make changes accordingly. Any optional step can be disabled, in which case that step will not appear in the application form.

The custom workflow is automatically activated upon creation.

All the steps configured in the product origination workflow will be part of the application form in the sequence defined.

The sequence, defined in the workflow that is active, will have an impact on bundled applications.

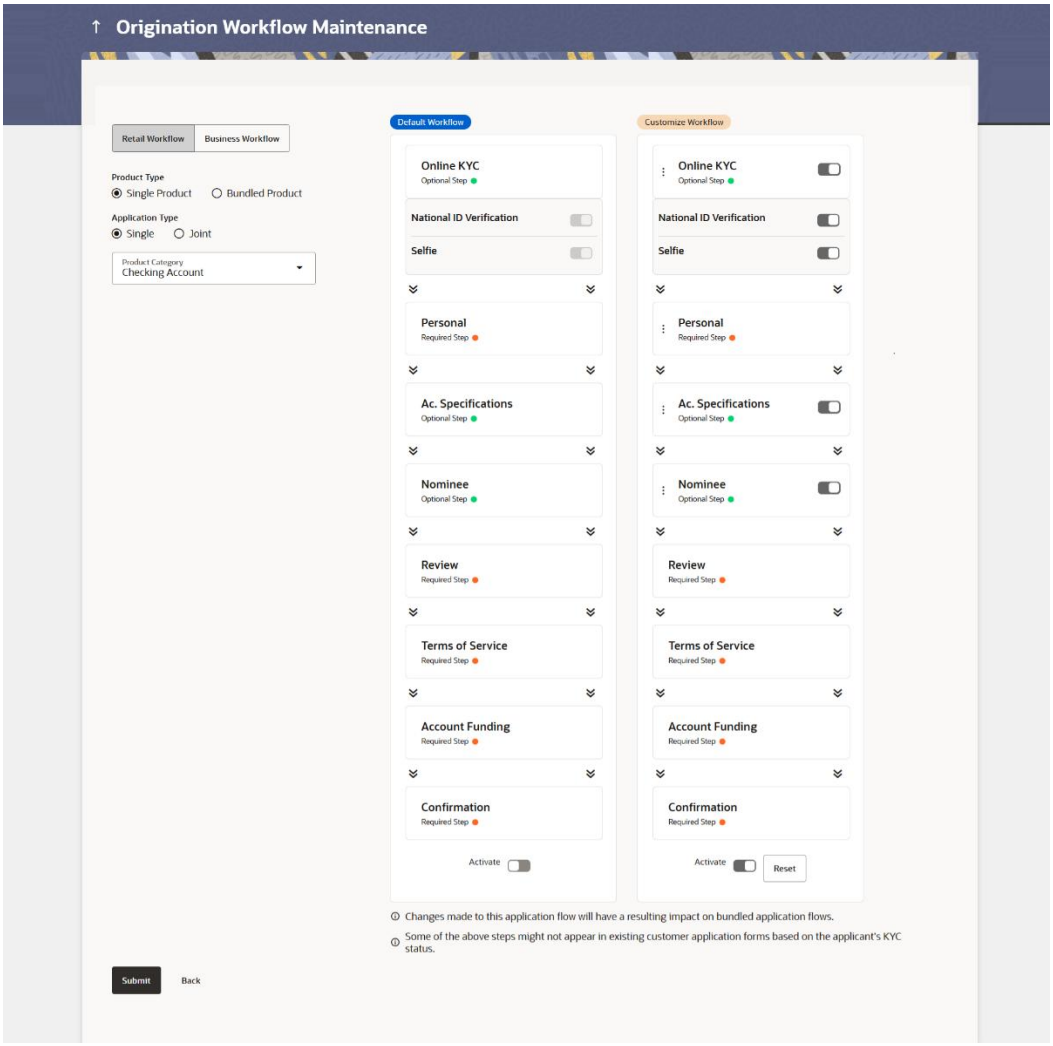
To edit the product application workflow:

1. The custom workflow is visible on the main screen adjacent to the default workflow.

   Click **Reset** to edit the workflow.

The workflow becomes editable and the administrator can rearrange the steps in the order as required and can also enable or disable Online KYC and if enabling Online KYC, can also define the mode to be enabled.

Origination Workflow Configuration - Customize Workflow



Field Description

Field Name	Description
Workflow Details	
Default Workflow	Default application workflow defined for the selected product category is displayed on the screen It depicts the sequence in which the sections of the application form will flow, if the default workflow is enabled.

Field Name	Description
Custom Workflow	Displays the customized application workflow for the selected product. Drag and drop blocks to customize the application workflow. The user can change the sequence of the steps and can also delete optional steps. Additionally the user can select the mode of Online KYC to be enabled or can also disabled Online KYC completely, if desired.
Activate	An activate button is present at the bottom of both the default and custom workflows. User can select to activate one of the workflows.
Reset	A reset button is provided below the custom workflow. This button resets all the changes to the custom workflow including re-ordering and deletion of steps and makes the custom workflow similar to the default workflow.

2. Click any card marked with the ⋮ icon and move the card to the position of choice.

Note: You can click icon and enable or disable the an optional step from the application flow if not required.

3. Click **Submit** to save the transaction.
   OR
   Click **Back** to navigate to the previous screen.
4. The success message of workflow creation appears as a toast message.

17.3 Bundle Application

Using this option, the Bank Administrator can create and maintain the priority to be assigned to each product category that can be part of a bundled application. This will dictate the sequence of steps within the bundled application form.

Based on the product category sequence, the workflows defined for each single or individual product application are considered to auto-generate the workflow for a bundled application. When the bundled application is initiated by the end-user, common sections across the different products will appear only once to the end-user. However, the steps that are unique to each product application will be sequenced based on the priority set as a part of bundled application only for the products selected by the customer in the bundle. Example:

Assume, the following is the workflow defined at each product category (defined using Single Product Application – custom flow) and the priority set against each product category (Defined using Bundled application – custom flow)

Checking Account	Personal Loan	Auto Loan
(Priority set in bundled application workflow - 1)	**(Priority set in bundled application workflow - 2)**	**(Priority set in bundled application workflow - 3)**

Upload Documents	Upload Documents	Upload Documents
Personal Information	Financial Profile	Home Loan Requirements
Account Specifications	Personal Loan Requirements	Personal Information
Review	Personal Information	Financial Profile
Terms of Service	Employment Information	Employment Information
Confirmation	Review	Review
	Terms of Service	Terms of Service
	Confirmation	Confirmation

Now assume that the guest user is applying for a bundled application consisting of one product from all the above three product categories from the digital platform. In this scenario, the sequence in which the information asked as a part of the application will be as follows:

1. Upload Documents
2. Personal Information
3. Account Specifications
4. Financial Profile
5. Personal Loan Requirements
6. Employment Information
7. Home Loan Requirements
8. Review
9. Terms of Service
10. Confirmation

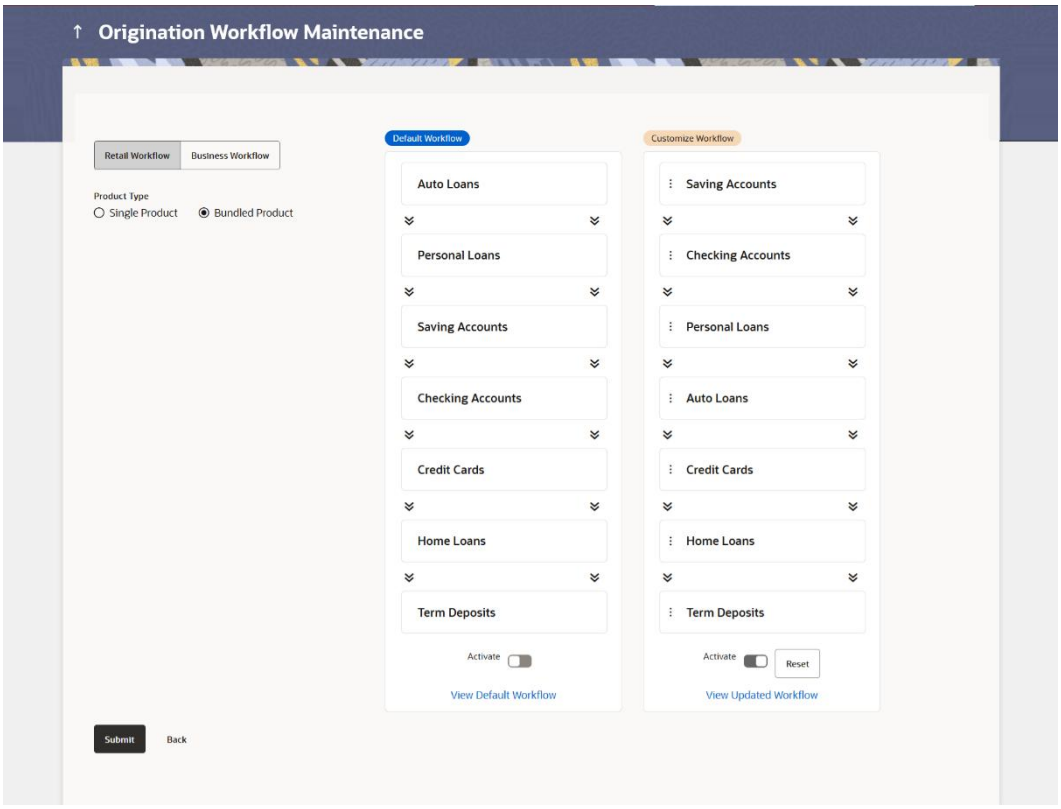
17.3.1 View Bundled Application Workflows

Using this option, the Bank Administrator can view the priority assigned to each product category that can be part of a bundled application. Apart from this, an option is provided to the bank administrator by way of which they can view the sequence in which the sections of a bundled application will flow considering different combinations of products that might make up the bundled application form.

To view the bundle application workflow:

1. In the **origination workflow configuration** page**,** select the product type as bundled application.
2. This opens both the default and the custom workflows for the bundled applications.

Bundled Product Application Workflow



Field Description

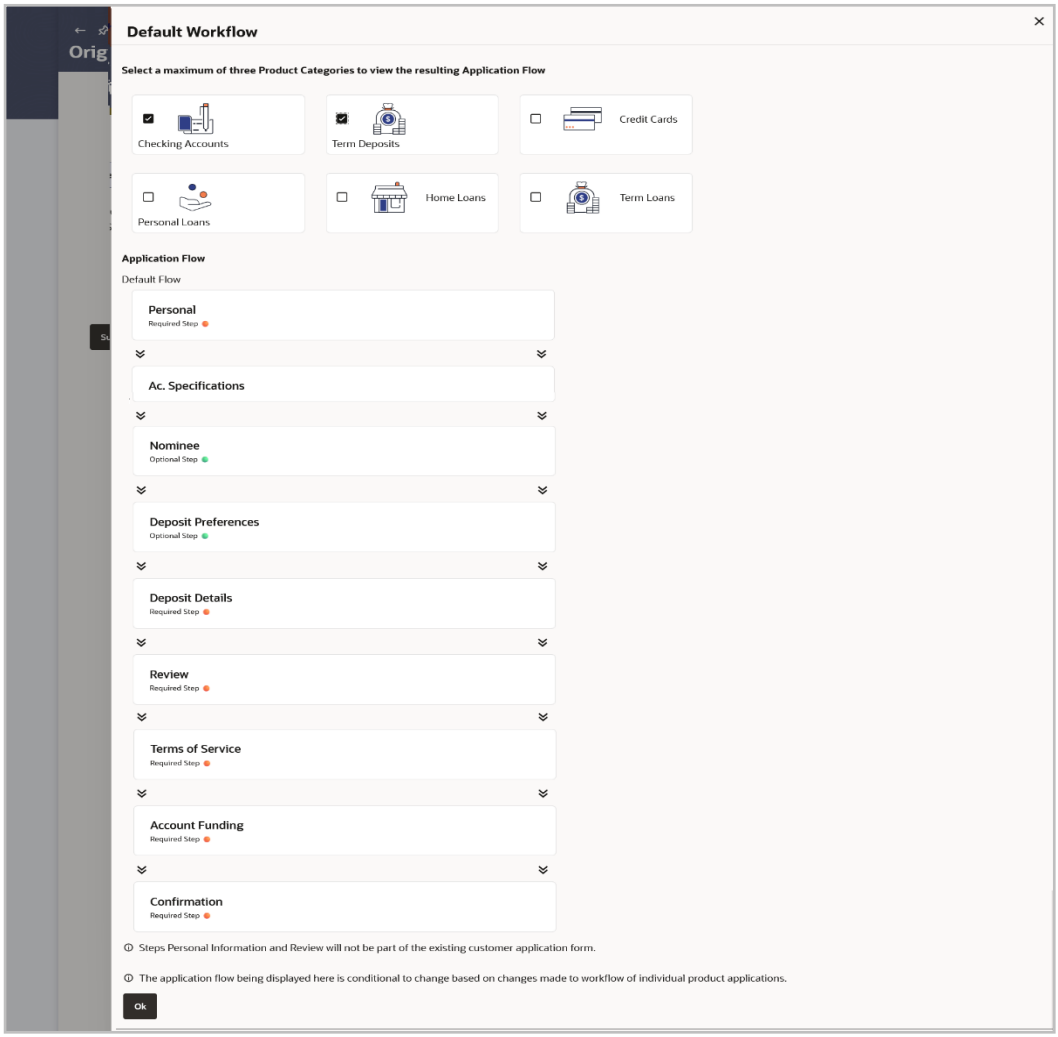
Field Name	Description
Product Priority for Bundled Application	
Default Workflow	Displays the default bundle application flow which specifies the product category priority offered by the bank.
View Default Workflow	Clicking on this option opens an overlay layer on which the administrator can select products so as to identify the sequence in which the sections of a bundled application will flow, if those products are part of a bundled application. The Bank Administrator can select any 2 or more product categories (maximum allowed in the bundle is 3 products).
Custom Workflow	Displays the customized bundled application flow. The user can change the product category priority as per their requirements.

Field Name	Description
View Updated Workflow	Clicking on this option opens an overlay layer on which the administrator can select products so as to identify the sequence in which the sections of a bundled application will flow, if those products are part of a bundled application. The Bank Administrator can select any 2 or more product categories (maximum allowed in the bundle is 3 products).

3. Click on the **View Default Workflow** link to view the product categories and application stages flow in bundle application. The **Default Application Flow** overlay screen appears.

   OR

Default Application Flow



Field Description

Field Name	Description
Product Categories	Displays the product categories offered by the bank in card form. The User can select the product categories to view the sequence in which the sections of the bundled application form will appear if these products are selected by the customer in the bundled application. The user can select maximum of 3 product categories.
Application Flow	Displays the default application flow for the bundle application that comprises of the selected product categories.

17.3.2 Edit Custom Workflow

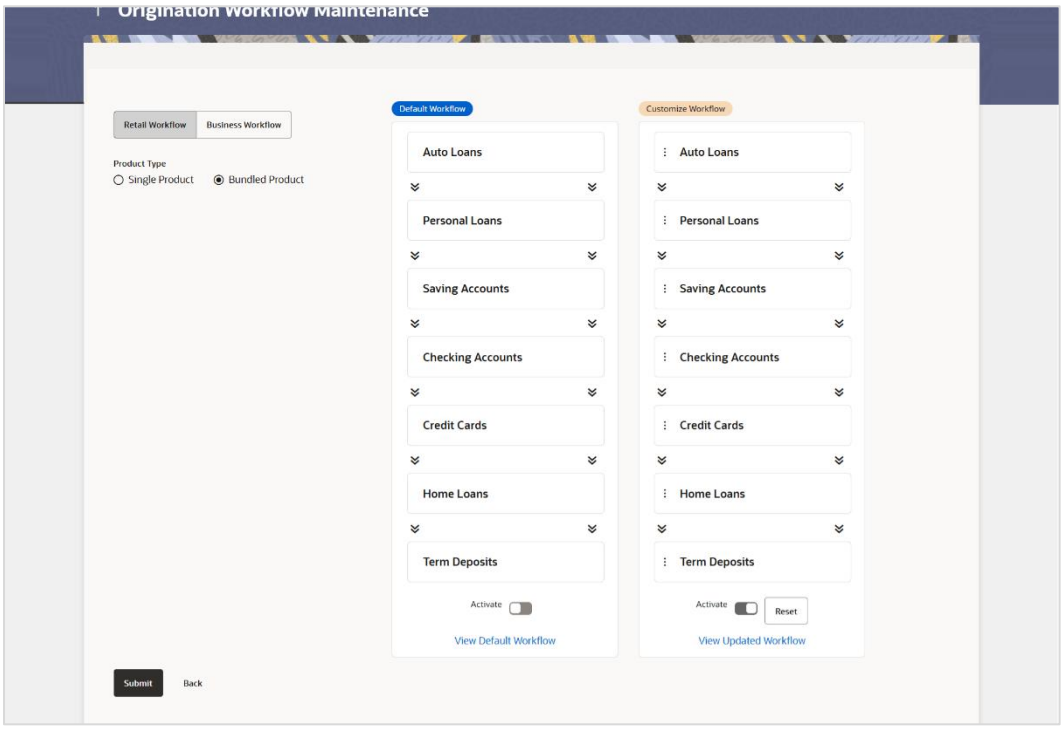
Using this option, the bank administrator can edit the custom bundled application workflow. The workflow will be automatically activated upon creation.

To edit the bundle application workflow:

1. The custom workflow is visible on the main screen adjacent to the default workflow.
2. Click any card marked with the ⋮ icon to move and rearrange the card where it needs to be placed in workflow.

Note: You can click icon and enable or disable the an optional step from the application flow if not required.

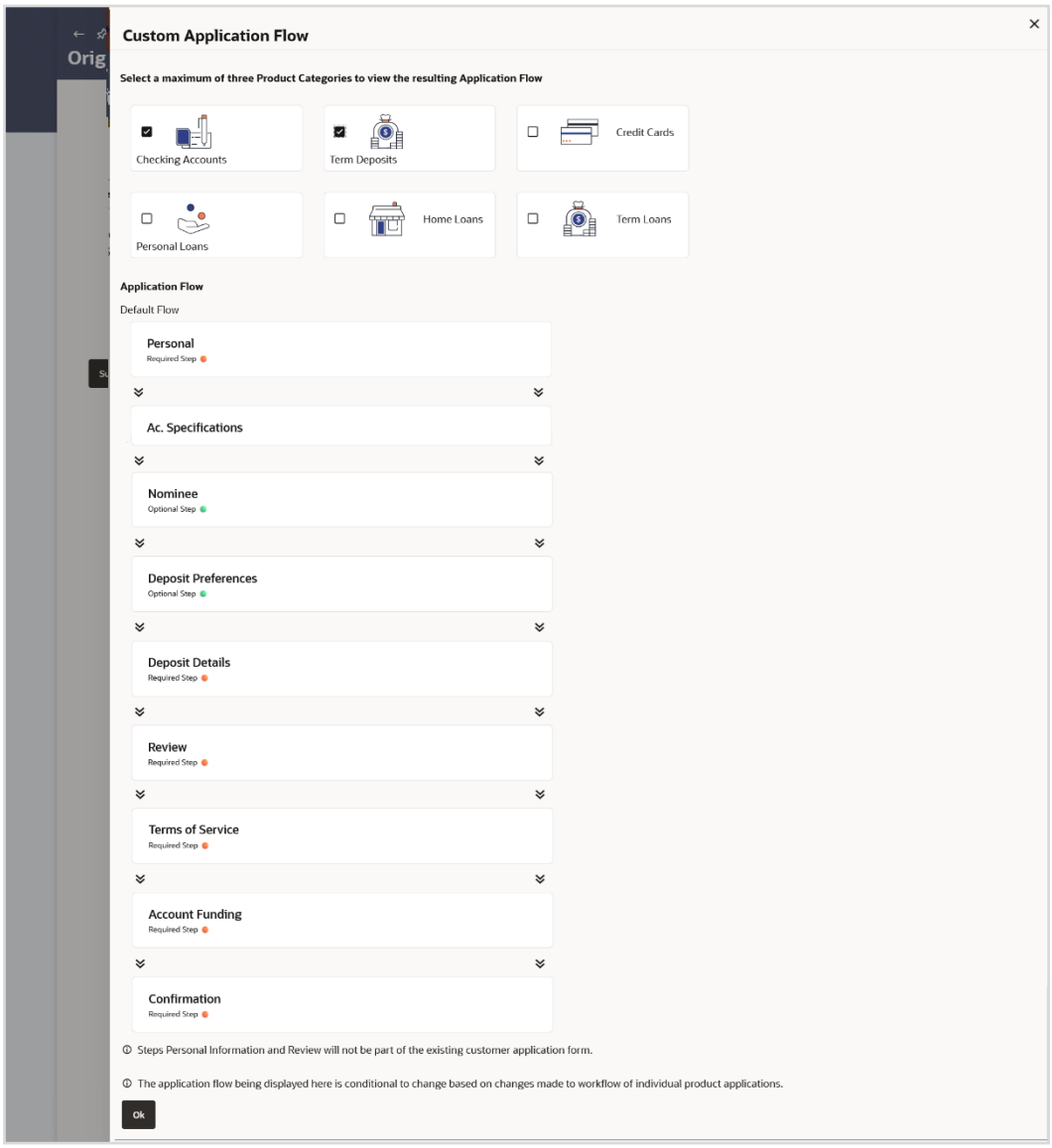
Edit Custom Workflow



3. Click on the **View Updated Workflow** link.

   The **Proposed Application Flow** overlay screen appears

Proposed Application Flow



Field Description

Field Name	Description
Product Categories	Displays the product categories offered by the bank in card form. The User can select the product categories to view the sequence in which the sections of the bundled application form will appear if these products are selected by the customer in the bundled application. The user can select maximum of 3 product categories.

Field Name	Description
Application Flow	Displays the default application flow for the bundle application that comprises of the selected product categories.

a. In the **Select Product Categories to see Application Flow** field, select the checkbox against the product category card which you wish to add in Bundle application, and whose application workflow to configured.

b. Click **OK** to add the product categories to bundle application.

Note: Click **Reset** to enable editing the workflow.

4. Click **Submit** to save the transaction.
   OR
   Click **Back** to navigate to the previous screen.
5. The success message of workflow creation appears as a toast message. n.

FAQ

1. **Do I have to activate the custom flow once created?**

Once the custom workflow is reset and edited, it becomes activated automatically.

2. **Is it mandatory to create a custom workflow?**

No. In case a customer workflow has not been created, the default workflow for that product category or bundled application will be in use.

3. **What will be the expected system behaviour if an optional step is enabled in a product category application workflow?**

If a step that is configured as optional, is enabled for a product category application workflow, it will appear in the sequence defined but will be optional i.e. the applicant will be able to skip the step without filling information in that step.

4. **What will happen to the applications which are in draft status with the old origination workflow?**

The application will be processed as per the new workflow defined by the banker. The information which is already filled by the customer will be pre-populated. In addition, user will be asked to provide the information if any as per the newly configured workflow.

5. **How many custom flows can I create per product category?**

Banker would be allowed to create only one custom flow. Modifications can be made in the custom flow at the later stage as per the bank's requirement.

6. **Can I configure the workflows at the product level available under each product category?**

No, as of now banker will be allowed to configure the workflows at product category level.

18. Product Maintenance

Product maintenance feature allows the System Administrator to map products to users from the channel.

System Administrator can map products maintained in the core banking system to different User type and all the users falling under that user type can open accounts for the mapped products only. This option is currently enabled for Term Deposit and Recurring Deposit module.

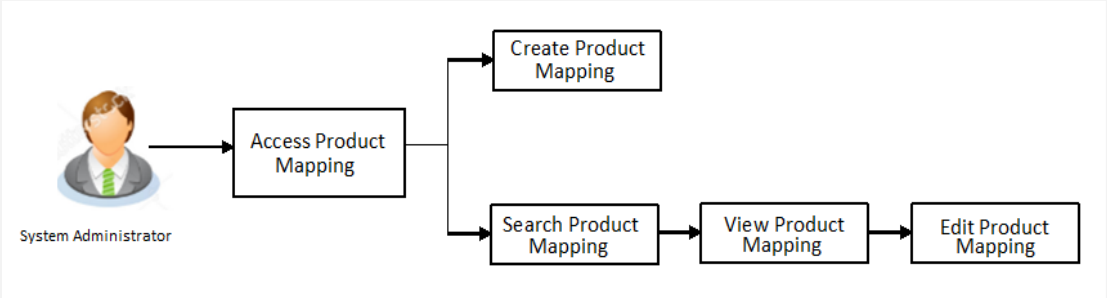
For example: A user can open a term deposit or a recurring deposit only under those products which are mapped to the User Type/Party Type/ User Segment assigned to the user. Products which are not mapped, will not be available (for opening deposit accounts) to a channel user. This will be a part of Day 1 setup.

Note: For User Type – Retail & Business, product mapping can be done for User Type, Party Type and User Segment combination.

Pre-Requisites

- Transaction access is provided to System Administrator.
- Approval rule is set up for System Administrator to perform the actions.
- Necessary products are maintained in core banking application.

Workflow



Features Supported In Application

The module supports following features:

- View Product Mapping
- Edit Product Mapping
- Create Product Mapping

How to reach here:

System *Administrator Dashboard > Configuration > Product Maintenance*
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Configuration > Product Maintenance

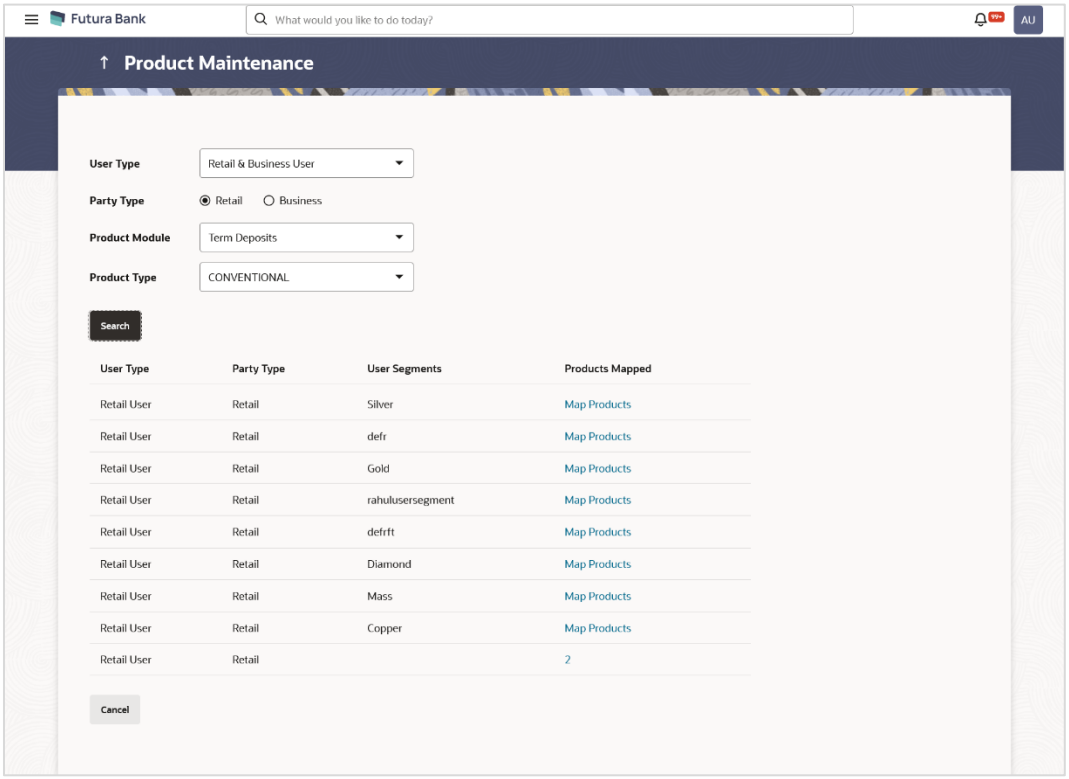
18.1 Product Maintenance - View

Using Product maintenance view option, System Administrators can view the list of products mapped to the product module. The System Administrator can view the mapping details by clicking the User Segments link.

To view the product mapping:

1. Navigate to the **Product Maintenance** screen. The **Product Maintenance** screen with mapped products appears.
   OR
   Click **Cancel** to cancel the transaction and navigate to the dashboard.

Product Maintenance



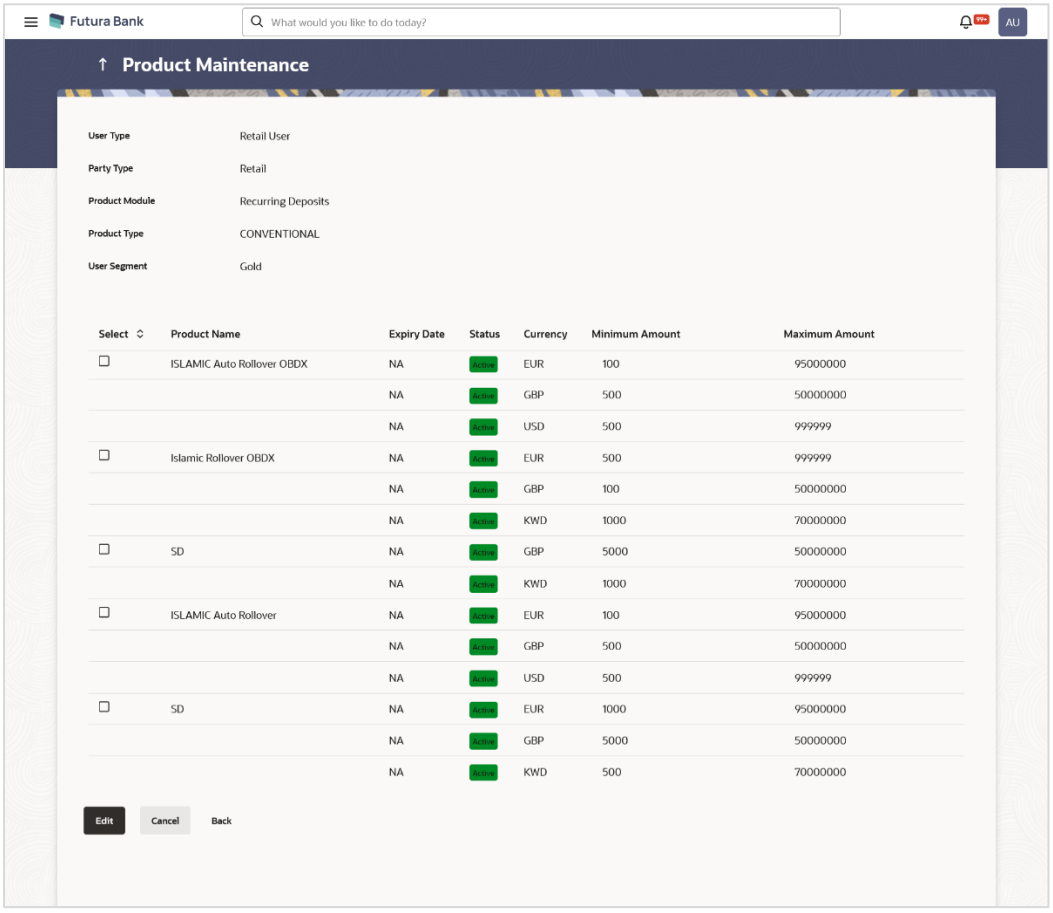
Field Description

Field Name	Description
User Type	The user type available for mapping products. The user types are “Corporate” and “Retail & Business”

Field Name	Description
Party Type	If the User Type is selected as “Retail and Business” then a new option Party Type is shown. The possible values are Retail and Business. Based on the party type selected, product mapping will be shown in the search results.
Product Module	Following product modules are available for mapping: • Term Deposit • Recurring Deposit
Product Type	The type of products available to be mapped to the user segment or to the role for that product module.
Search Result	
User Type	The user for which products are mapped.
Party Type	The Type of party for the user. Applicable only for user type Retail & Business user
User Segment	The user segments for which products mapped. This field is applicable only for Retail user type.
Products Mapped	The number of products mapped to the user segment or user type for that product type and product module.

2. Click the **Product Mapped** link of the user record for which you want to view the details. The **Product Mapping - View** screen appears.

Product Maintenance - View



Field Description

Field Name	Description
View	
User Type	The user for which products are mapped.
Party Type	The Type of party for the user. Applicable only for user type Retail & Business user
Product Module	Following product modules are available for mapping: • Term Deposit • Recurring Deposit Note: For corporate only Term Deposit product module is available

Field Name	Description
Product Type	The type of product under the selected module for which the product list needs to be fetched .
User Segment	The user segment for which products are mapped. This field is applicable only for Retail user type.
Product Name	Name of the product which is mapped to the user type for the selected product type and product module.
Expiry Date	The expiry date of the product. If the product is expired, an 'Expired' flag is shown against the product.
Status	The current status of the product.
Currency	The currency in which products are maintained.
Minimum Amount	The minimum permissible amount for opening deposit under the selected product.
Maximum Amount	The maximum permissible amount for opening deposit under the selected product.

3. Click **Edit** to edit the user-segment - product mapping.
   OR
   Click **Cancel** the operation and navigate to the 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.

18.2 Product Maintenance - Edit

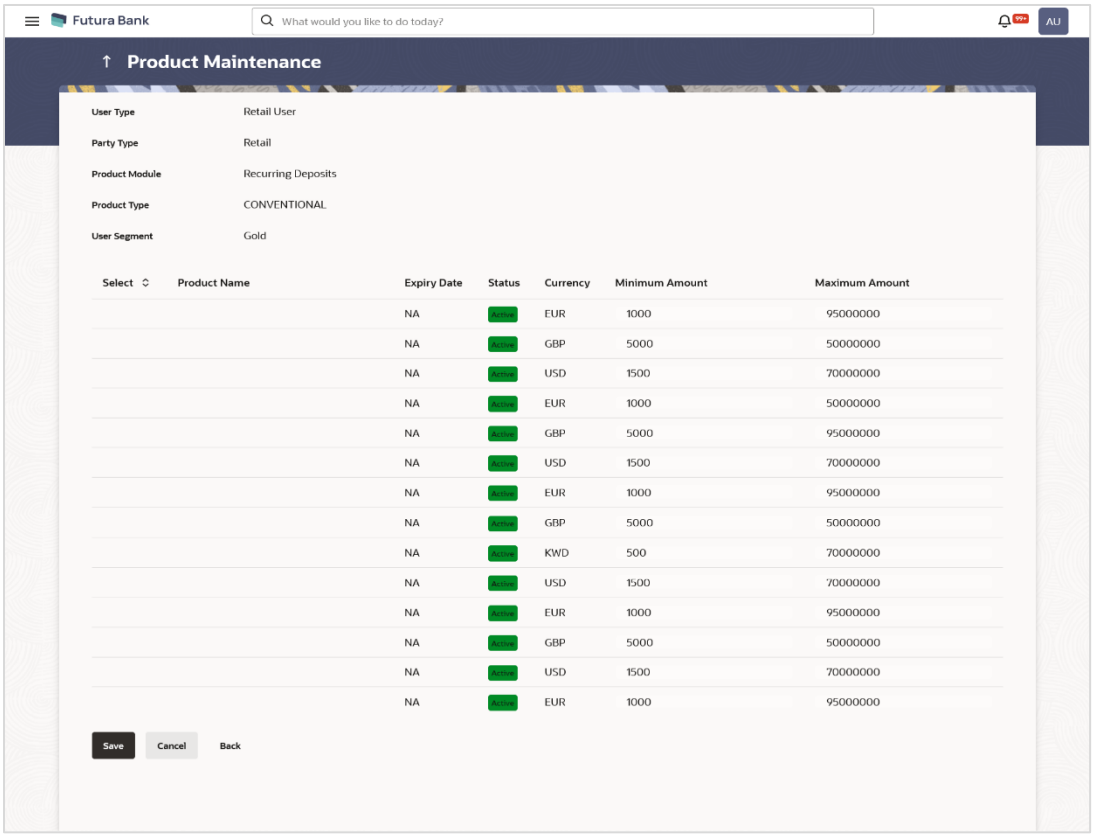
This function enables the System Administrator to edit the product mapping. The System Administrator can map or delete the products to the product module.

To edit or update the product mapping:

1. In the **Product Maintenance** screen, click the **Product Mapped** link of the user record for which you want to edit the details.
   The **Product Maintenance - View** screen appears.

2. Click **Edit** to edit the user-segment - product mapping. The **Product Mapping – Edit** screen appears.
   OR
   Click **Cancel** the operation and navigate to the ‘Dashboard’.
   OR
   Click **Back** to navigate to the previous screen.

Product Maintenance - Edit



Field Description

Field Name	Description
Edit	
User Type	The user for which products are mapped.
Party Type	The Type of party for the user. Applicable only for user type Retail & Business user

Field Name	Description
Product Module	One of the following product modules for which the mapping is to be edited: • Term Deposit • Recurring Deposit
Product Type	The list of product type, available for mapping.
User Segment	The user segment, for which products are mapped.
Product Name	Name of the product which is mapped to the user type for the selected product type and product module.
Expiry Date	The expiry date of the product. If the product is expired, an 'Expired' flag is shown against products.
Status	The current status of the product.
Currency	The currency in which products are maintained.
Minimum Amount	The minimum permissible amount for opening deposit under the selected product.
Maximum Amount	The maximum permissible amount for opening deposit under the selected product.

3. Edit View the defined values for fields, in an editable form.
4. Edit the required details.
5. Click **Save** to save the changes.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to navigate to previous screen.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
7. The success message of transaction submission appears along with the transaction reference number and status.
   Click **OK** to complete the transaction.

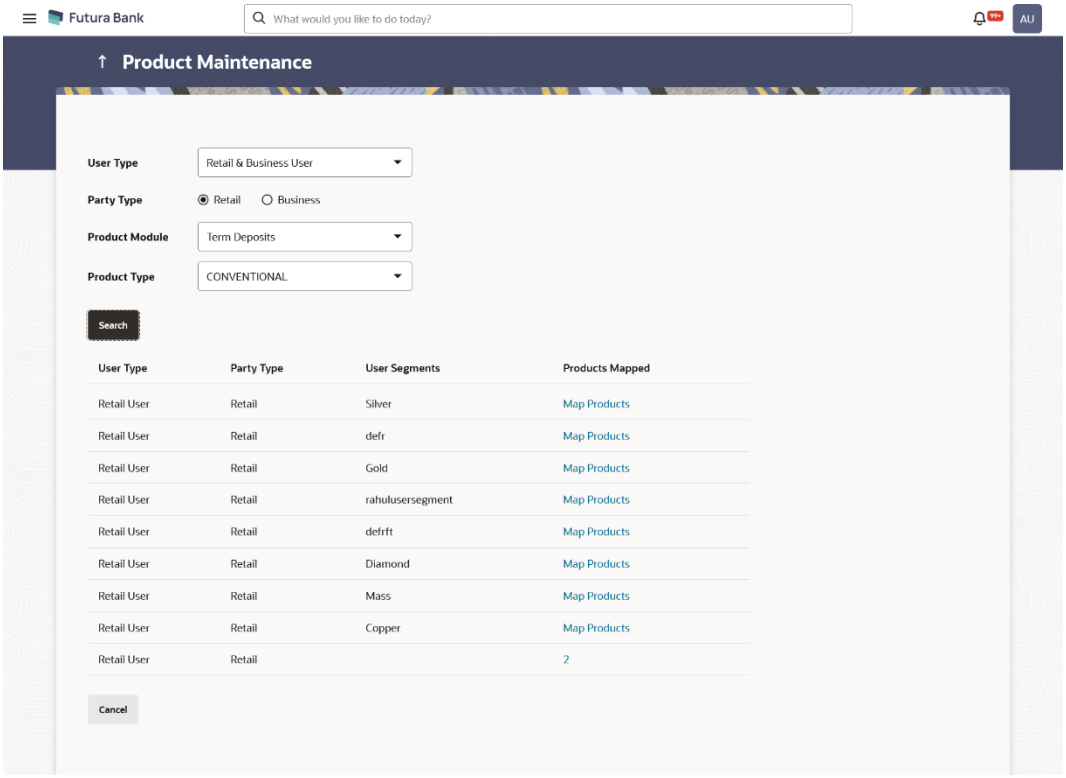
18.3 Product Maintenance - Create

This option enables the System Administrator to select the products and map it to the Product Module.

To create a new product mapping:

1. Navigate to the **Product Maintenance** screen.
2. Select the User Type for which the product mapping needs to be maintained
3. Select the Party Type (if applicable) for which the product mapping needs to be maintained
4. Select the User Segment (applicable only for Retail user type).

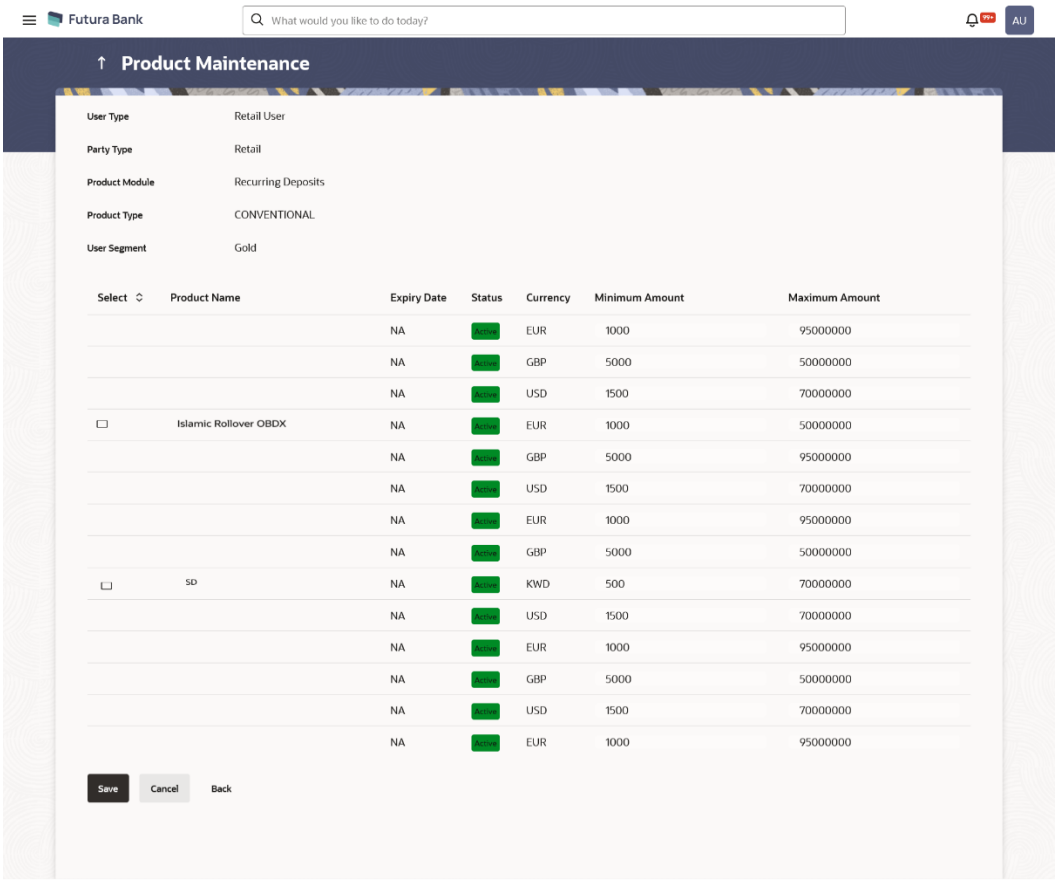
Product Maintenance



5. Click **Map Products**.
   The **Product Maintenance - Create** screen appears.

Note: The **Map Products** link is available only if no products are mapped to the user segment.

Product Maintenance - Create



Field Description

Field Name	Description
Create	
User Type	The user for which products are mapped.
Party Type	The Type of party for the user. Applicable only for user type Retail & Business user
Product Module	Following product modules are available for mapping: • Term Deposit • Recurring Deposit
Product Type	The list of product, available for mapping.
User Segment	The user segment, for which products are to be mapped.

Field Name	Description
Product Name	Name of the product which is mapped to the user type for the selected product type and product module.
Expiry Date	The expiry date of the product. If the product is expired, an 'Expired' flag is shown against products.
Status	The current status of the product. **Note**: Only the active products are displayed
Currency	The currency in which products are maintained.
Minimum Amount	The minimum permissible amount for opening deposit under the selected product.
Maximum Amount	The maximum permissible amount for opening deposit under the selected product.

6. From the **User Type** list, select user for which products are mapped.
7. From the **Product Module** list, select product modules which are available for mapping.
8. From the Product Type list, select product type available for mapping.
9. Select the checkbox(s) for the product which has to be mapped to the user.
10. In the Minimum Amount field, enter the minimum permissible amount for opening deposit under the selected product.
11. In the Maximum Amount field, enter the maximum permissible amount for opening deposit under the selected product.
12. Click Save to save the mapping.
    OR
    Click Cancel to cancel the operation and navigate back to ‘Dashboard’.
    OR
    Click Back to navigate to previous screen.
13. The Review screen appears. Verify the details, and click Confirm.
    OR
    Click Cancel to cancel the transaction.
    OR
    Click Back to navigate to previous screen.
14. The success message of transaction submission appears along with the transaction reference number and status.
    Click OK to complete the transaction.

FAQ

1. **For which type of products, product mapping functionally is available?**

As of now, product mapping feature is enabled only for Term Deposit and Recurring Deposit type of products for retail users and Term Deposit for corporate users.

2. **Can customer view the account details of an account opened under a product which is not mapped?**

Yes, user can view the account details of an account opened under a product which is not mapped. The restriction will only be for opening new account from channel.

3. **What will happen once the products mapped gets expired?**

The expired products will no longer be available for product mapping. Also customers will not be able to open new accounts using expired product.

4. **What will happen if the products are not mapped to any user segment and are only mapped to user type?**

In this case, all the products mapped to the user type will be available for account opening to the users associated to that user type.

19. Analytics Dashboard

The analytics dashboard provides insight into digital banking platform usage patterns and customer trends. It helps the bank's product managers to gain a complete understanding of how products are used, helps improve decision-making by providing easy performance indicators, and keep track of progress over a period of time. It presents key metrics neatly on a user interface that shows trends and changes in data over time.

An option to download the information presented on the screen is also provided.

Following KPIs (Key Performance Indicator) and widgets are displayed in on the Analytics Dashboard:

KPIs:

- Total Users
- Active Users
- Logins
- Average Transactions
- Average Time Spent

Widgets:

- Total Users
- User Status
- Users by Touch Points
- Segment Distribution
- Business User Statistics
- User logins by devices
- User Activity
- Device Preferences
- Age wise Primary Touch points Usage
- Top 20 Transactions

How to reach here:

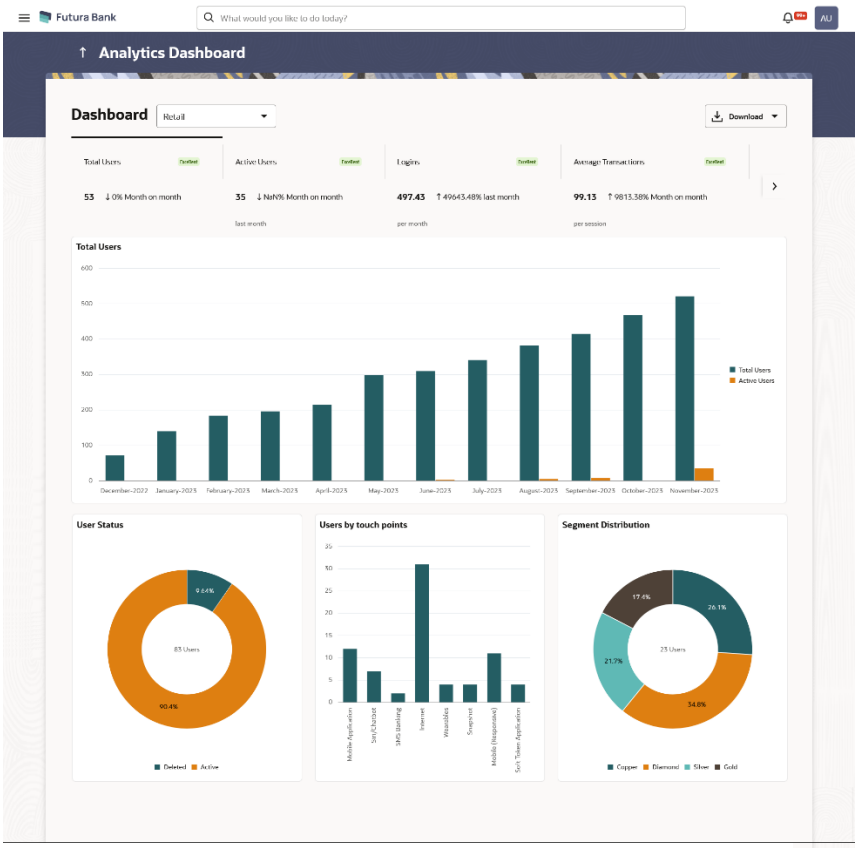
System/ Bank Administrator Dashboard > Toggle menu > Menu > Controls & Monitoring > Analytics Dashboard
OR
Search bar > Controls & Monitoring > Analytics Dashboard

To view analytic dashboard:

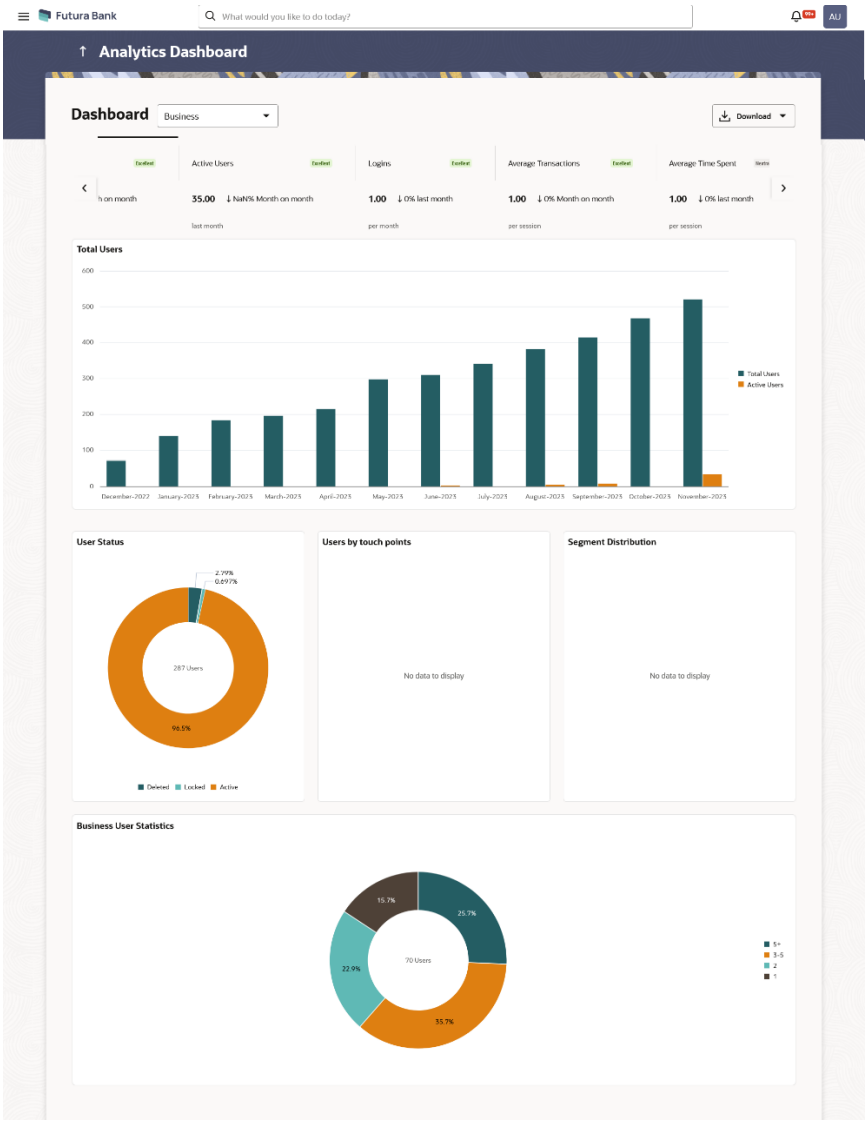
1. Navigate to the screen, the **Analytics Dashboard** screen appears.

2. Select the user type from the drop-down list. The search results appears based on the selected user type. By default Retail user and the KPIs/Widgets associated with it appear.

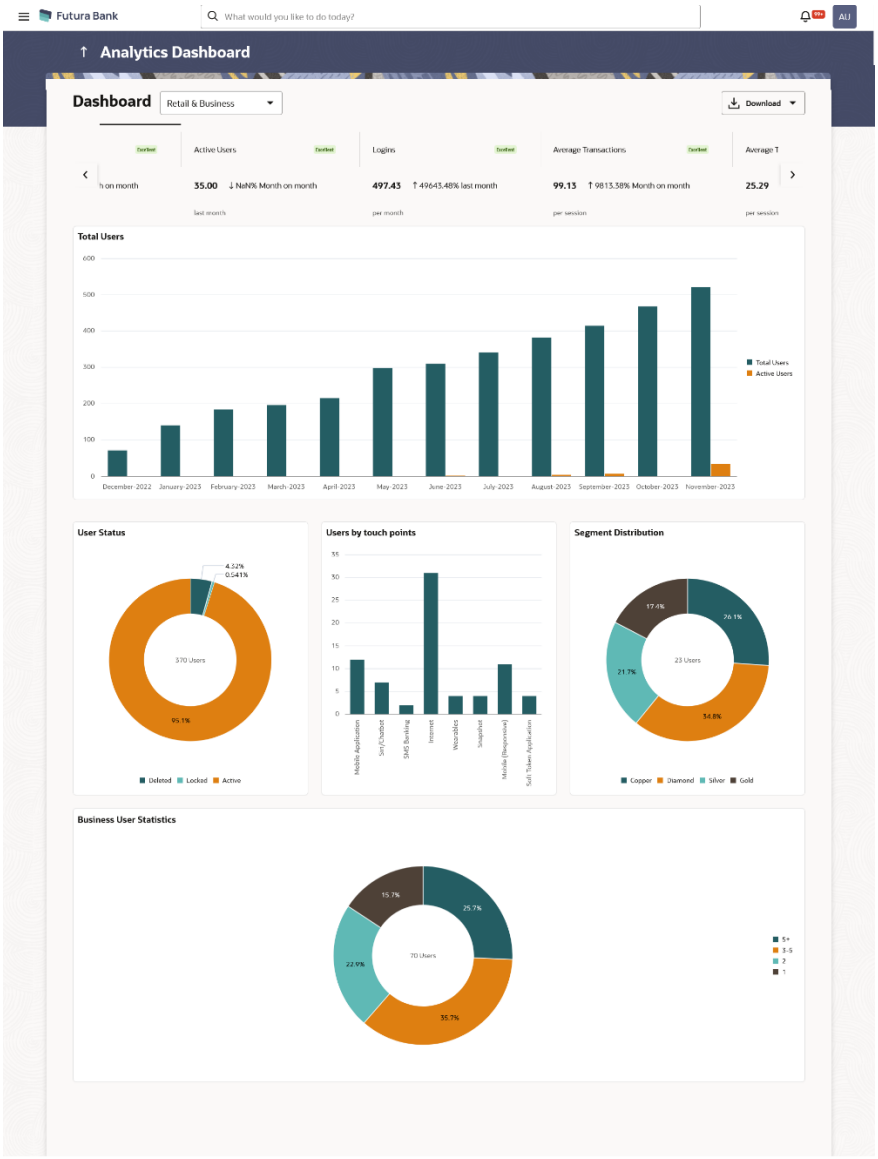
Analytic Dashboard – Retail User



Analytic Dashboard – Business User



Analytic Dashboard – Retail & Business User



Field Description

Field Name	Description
User Type	Type of user. The user can be: • Retail • Business • Retail & Business

Field Name	Description
Following are the widgets gets displayed on dashboard	
KPIs	
Following are the different performance indicators shown	
Total Users	This card displays change in total users on month-by-month basis (in %), and the status based on that.
Active Users	This card displays the change in active users in the last month on a month-by-month basis (in%) and the status based on that.
Logins	This card displays the change in total number of logins (in %) per month in comparison to the last month, and the status based on that.
Average Transactions	This card displays the average transactions performed per session on month-by-month basis (in %), and the status based on that.
Average Time Spent	This card displays the average time spent to complete a task for transactions by user in comparison to the last month (in %), and the status based on that.
Status	The status displayed on performance indicators. The options are: • Excellent - > +10% • Good – between +5% and +10% • Neutral – between -5% and +5% • Warning - between -10% and -5% • Critical - >-10%
Widgets	
Total Users	This graph provides a quick snapshot of the total users and active users in the last 12 months. The user can view the more information in each month by hovering over each slice of the graph.
User Status	This widget displays the allocation of different users (in %) in donut graph form. It provides view of the deleted users and active users with respect to total number of users. The user can view detailed information by hovering over a donut graph in each slice.

Field Name	Description
Users by touch points	This graph provides a quick snapshot of the total users with respect to some selected touch point. The user can view the more information in each touch point by hovering over each slice of the graph.
Segment Distribution	This widget displays the allocation of different users as per the segment (in %) in donut graph form. The user can view detailed information by hovering over a donut graph in each slice.
Business User Statistics	This widget displays the number of users per business (in %) in donut graph form.
User Logins by Devices	This chart enables the users to track the distribution of user logins across different devices and mostly used touch points for selected quarter. The user can view the more information in each device by hovering over each slice of the graph.
User Activity	This widget helps identify the users logins frequency for the selected quarter. The user can view detailed information by hovering over a donut graph in each slice.
Device Preferences	The bank can identify the users who are using the multiple devices for accessing the platform their banking needs. The user can view detailed information by hovering over a donut graph in each slice.
Age wise Primary Touch Points Usage	The users can explore the age-wise device usage trends using this widget. The user can view detailed information by hovering over a donut graph in each slice.
Top 20 Transactions	This widget enables the user to gain insights into the most widely used transactions, providing a snapshot of user behaviour while accessing the banking services through channel banking platform. The user can view the more information in transaction listed by hovering over each slice of the graph.

3. Click **Download** to download the details report in pdf & CSV format.

FAQ

1. **Can the user modify the widget, KPIs or change the parameters on which the graph will be plotted?**

   Though the option has been provided to the bank users to select the date ranges to get the desired details for certain widgets for the selected period; these widgets, KPIs or filter criteria cannot be modified using configuration. However configuration properties has been provided for modification of the KPI performance indicators from back-end.

20. Resource Bundle Maintenance

Resource bundles contain locale-specific objects. When your program needs a locale-specific resource, a String for example, your program can load it from the resource bundle that is appropriate for the current user's locale.

These Resource bundles are maintained inside digx_fw_resource_bundle table. We have grouped these bundles based on modules inside digx_fw_resource_bundle_mapping table.

At a time any single resource from these bundles can be selected at this screen and its Resource values/display names for corresponding supported user locale can be updated simultaneously (bulk update).

Features Supported In Application

This option allows the System Administrator to:

- Search Resource Bundle
- View Resource Bundle
- Edit Resource Bundle

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Configuration > Resource Bundle Maintenance
OR
Search bar > Configuration - Resource Bundle Maintenance

20.1 Resource Bundle Maintenance - Search & View

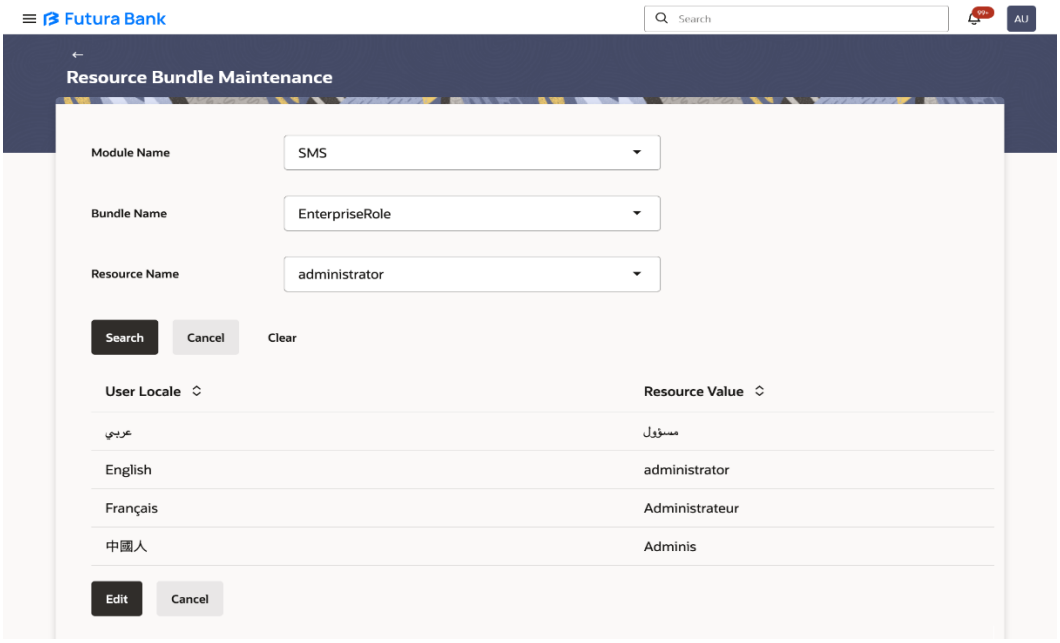
Bank Administrator can search existing resource bundle maintained based on the module name, resource name and bundle name.

To search and view the Resource Bundle:

1. Navigate to the **Resource Bundle Maintenance** screen.
2. From the **Module Name** list, select the module name by which you wish to search resource.
3. From the **Bundle Name** field, select the bundle name by which you wish to search resource.
4. From the **Resource Name** list, select the resource name by which you wish to search resource.
5. Click **Search**. Based on selected Resource Name a table containing all the available user locales and their corresponding resource display names for that resource will appear.

OR
Click **Cancel** to cancel the transaction.
OR
Click **Clear** to reset the data entered.

Resource Bundle Maintenance – Search Result



Field Description

Field Name	Description
Module Name	Specify the module by which you wish to search resource.
Bundle Name	Specify the bundle from bundles mapped to selected Module by which you wish to search resource.
Resource Name	Specify the resource from resources mapped to selected Bundle by which you wish to search resource.
Search Results	
User Locale	Displays the all User locale supported by the system.
Resource Value	Displays the Resource Display Name corresponding to User Locale for that Resource Name.

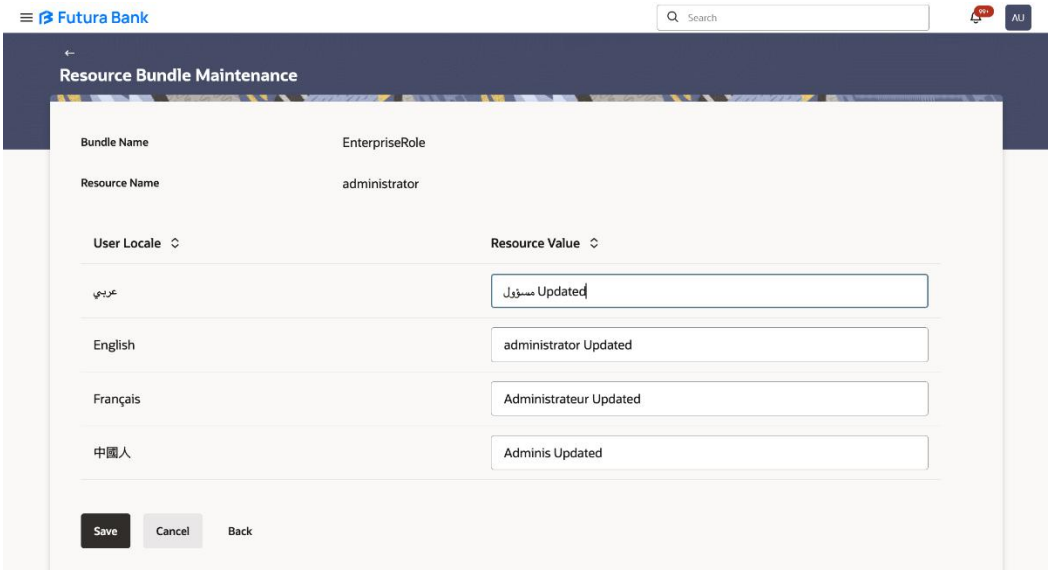
20.2 Resource Bundle Maintenance - Edit

Using this option, the administrator can simultaneously update all Resource Values corresponding to all user Locales for selected resource.

To edit or modify resource bundle:

1. Search the resource bundle by specifying search criteria and click **Search**. The system displays the list of all User Locale and their corresponding Resource Values for selected Resource Name.
2. Click **Edit** against the record to update the locale specific resource value.

Resource Bundle Maintenance – Edit



3. Click **Save** to update the changes.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
4. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to go to previous screen.
5. The success message with reference number & status appears.
   Click **OK** to complete the transaction.

21. Feedback

Customer experience and satisfaction are very important aspects for the banks and it differentiates one bank from another, hence measuring customer satisfaction is exceedingly important. Feedback capture allows the customers to express their opinion on the services offered by the bank.

The following capabilities are available as part of feedback:

- Feedback Template definition
- Feedback capture on transaction completion
- General Feedback capture
- Feedback Analytics

As part of feedback template definition, the administrator can define the feedback question, the rating scale, question and option set along with deciding the set of transaction(s) for which feedback capture needs to be enabled.

The business users i.e. retail and corporate users will get an option to capture feedback on completion of transaction depending upon whether the transaction is part of the feedback template applicable to the role of the user.

The business user also has an option to capture general feedback if required and not necessarily perform a transaction to capture feedback.

Feedback captured by the user in terms of the rating and the options selected on the subsequent questions asked are stored in the system for the bank to carry out analysis for corrective actions if required. The administrator will have an option to view the details.

21.1 Feedback Template Maintenance

Using this option, the System Administrator can maintain the feedback templates by defining the feedback question, selecting the rating scale, adding new questions along with new options, selecting the transactions for which feedback capture needs to be enabled.

The administrator can also decide whether an additional question is to be asked for a scale weight and select the applicable options for the question.

How to reach here:

System Administrator Dashboard > Templates > Feedback Template
OR
Bank Administrator Dashboard > Others > Feedback
OR
System / Bank Administrator Dashboard > Toggle Menu > Menu > Templates > > Feedback Template

21.1.1 Feedback Template Maintenance - Search

To search feedback template:

1. In the **Template ID** field, enter an appropriate template ID if you wish to search by template ID.
2. In the **Template Name** field, enter the name of the template to be searched.
3. Select appropriate role(s) if you wish to search the template based on the parameter **Applicable to Role**.
4. Click **Search**.

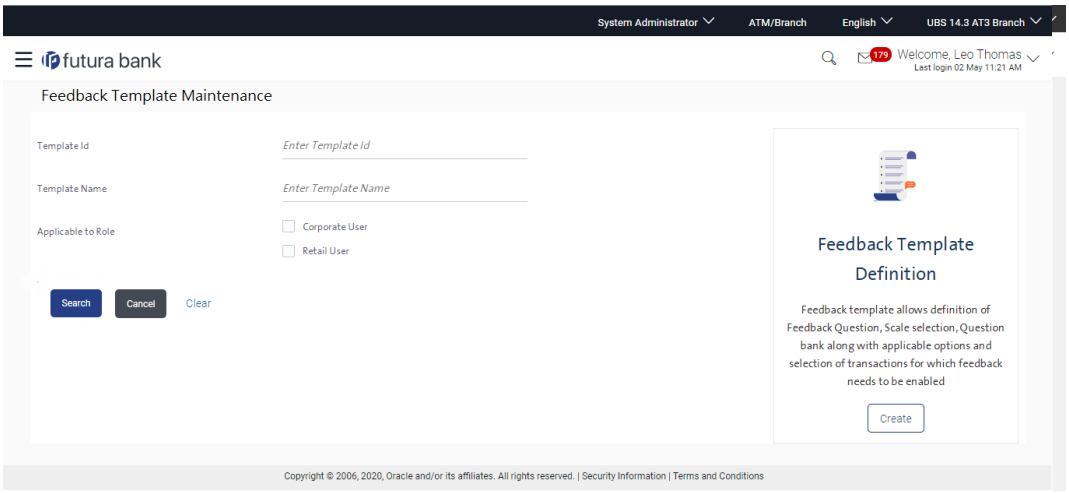
   OR

   Click **Clear** to reset the search parameters

   OR

   Click **Cancel** to cancel the transaction

Feedback Template Maintenance-Search



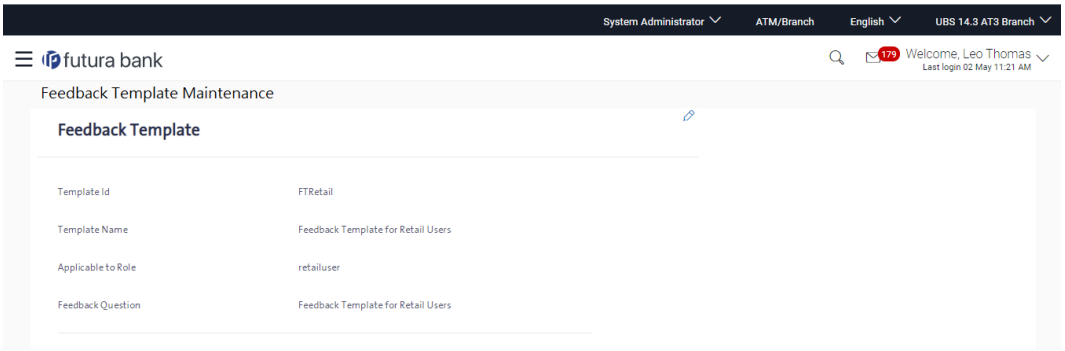
Field Description

Field Name	Description
Template ID	Specify the template ID you want to search.
Template Name	Specify the template name you want to search.
Applicable To Role	Select the role if you wish the search the template based on the role.
Search Results	

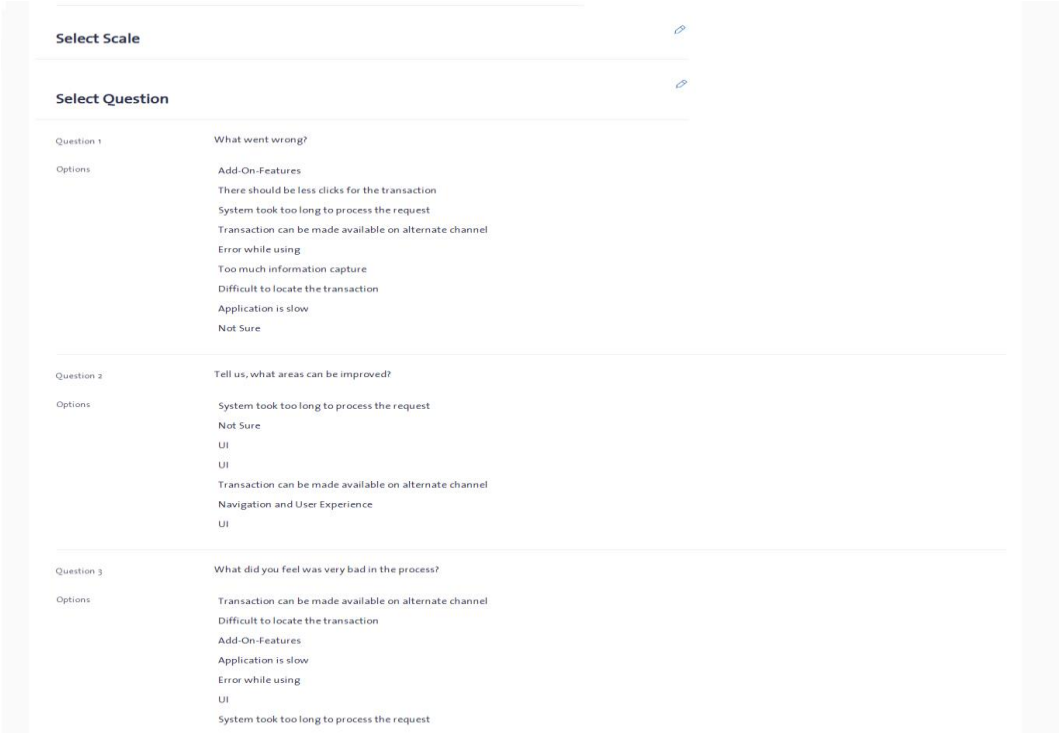
Field Name	Description
Template ID	Displays the template ID of the applicable template based on the search criteria.
Template Name	Displays the template name of the applicable template based on the search criteria.
Applicable To Role	The role to which the searched feedback template is applicable.

5. Click the link under the **Template ID** column. The **Feedback Template Maintenance** screen appears with the details of the feedback template i.e. template ID, template name, feedback question, question and option set along with the set of transactions for which template is applicable.

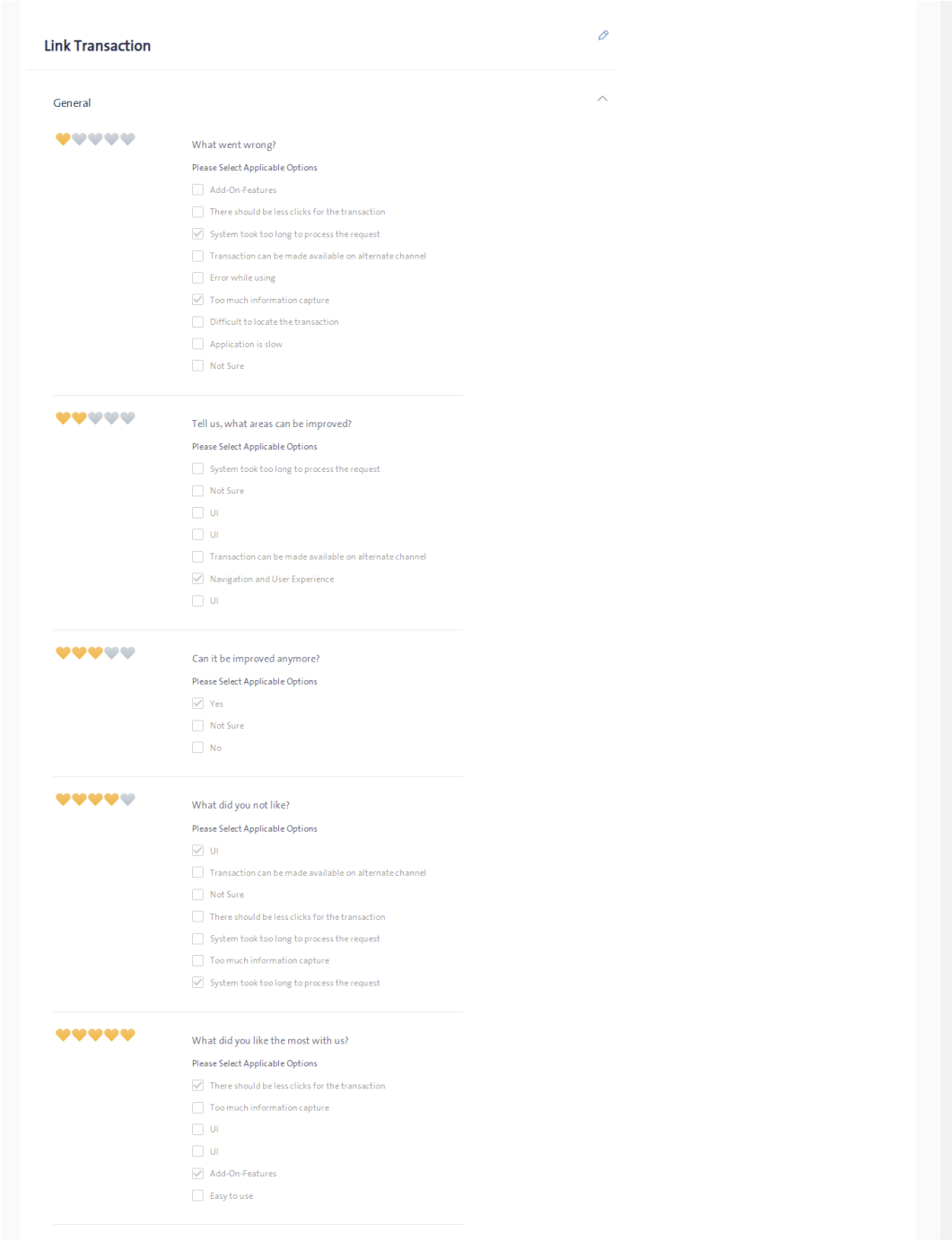
Feedback Template – View

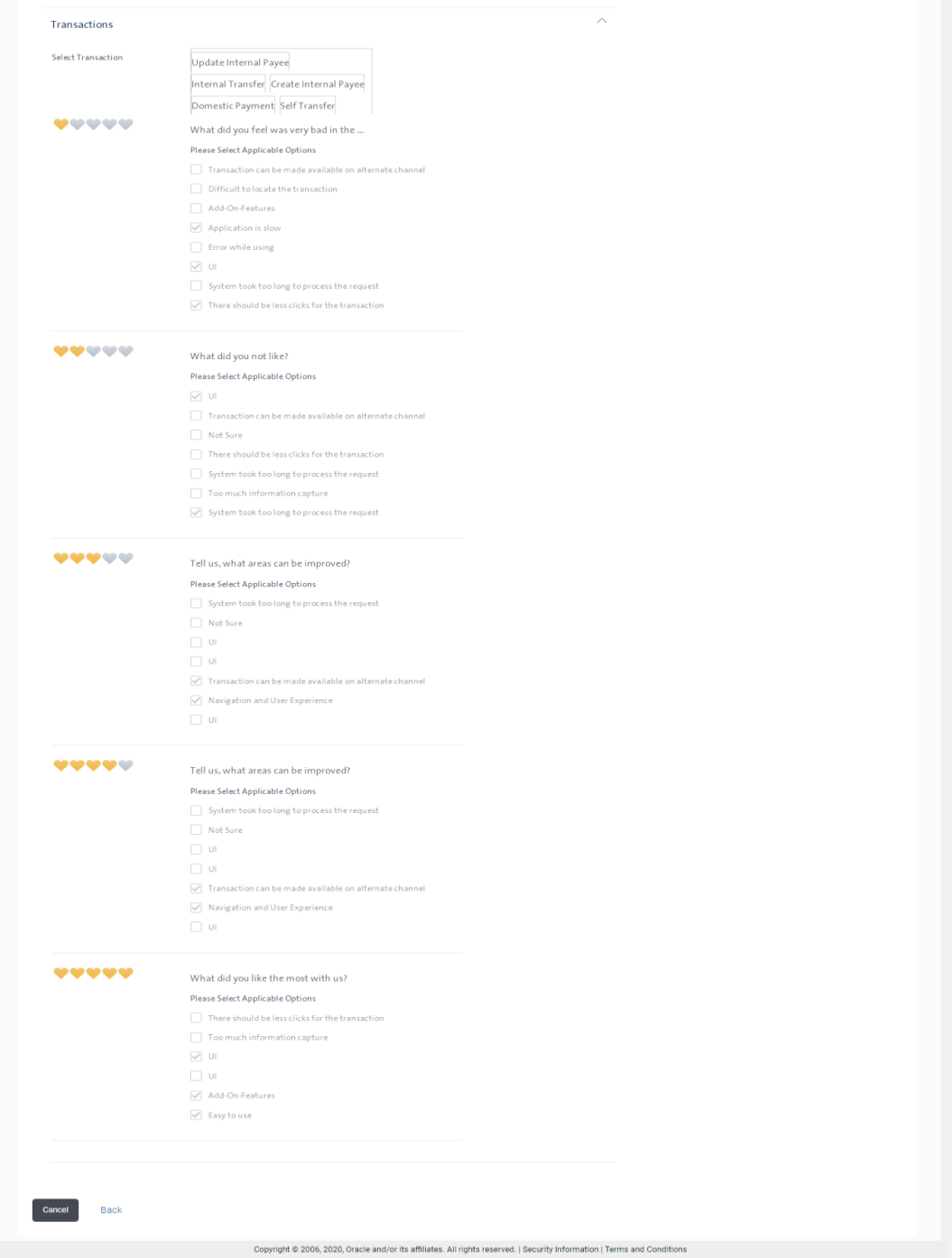


Select Scale – View



Link Transaction – View





6. Click against the respective section to edit the feedback template.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

21.1.2 Feedback Template Maintenance - Edit

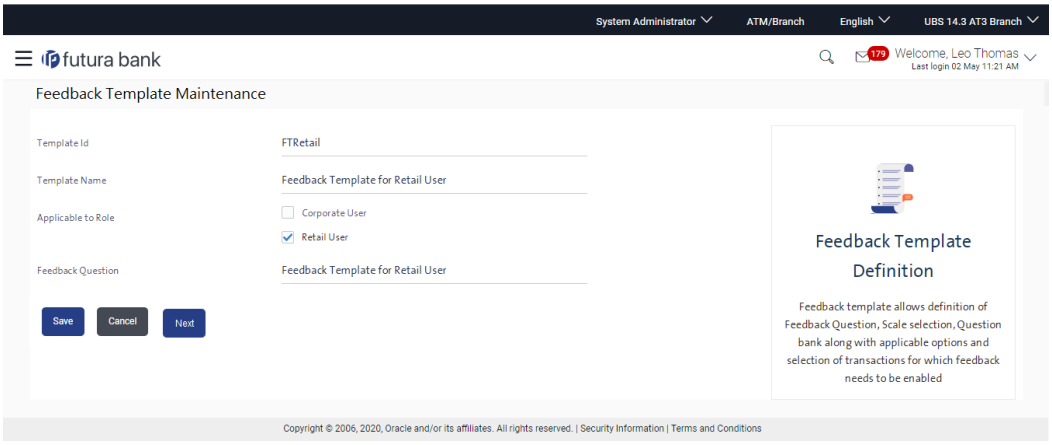
Using this option, the administrator can modify details in the feedback template i.e. update feedback question, change the rating scale, add new questions and options, add / remove transactions from the template.

To edit or modify feedback template:

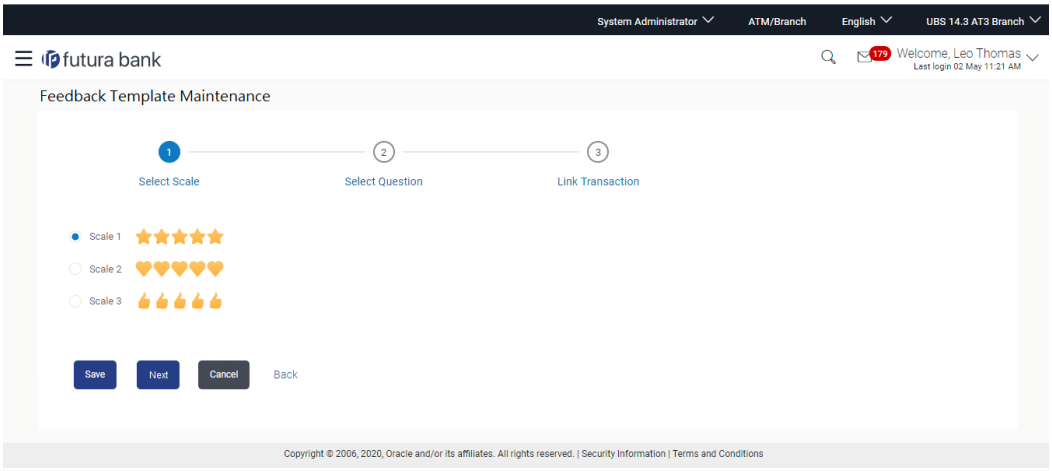
6. Search the Feedback template by specifying different search criteria and click **Search**. The search results appear on the **Feedback Template Maintenance** screen based on the search parameters.
7. Click the link under the **Template ID** column. The **Feedback Template Maintenance** screen appears.
8. Click to edit the details in respective section of the feedback template. The **Feedback Template Maintenance - Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
9. The administrator will be navigated to the respective section i.e. feedback template details or scale definition or select question or link transaction depending on the edit option selected against the respective section.
10. As part of feedback template details, feedback question, template ID, template name and applicable to role can be modified
11. As part of scale definition, the administrator can change the rating scale
12. As part of select question section, the administrator can add new questions and also add new options for existing as well as new questions defined.
13. As part of link transaction section, the administrator can add new transactions as well as remove existing transactions.

    Administrator can also add new options, to the existing questions associated to each scale weight of the rating scale applicable to general feedback as well as for transactions
14. Edit the required details in the respective section and click **Save** if you need to go to review page
    OR
    Click **Next**, to go to the next step in the process and edit details wherever required.
    OR
    Click **Back** to go to the previous page.
    OR
    Click **Cancel** to cancel the transaction

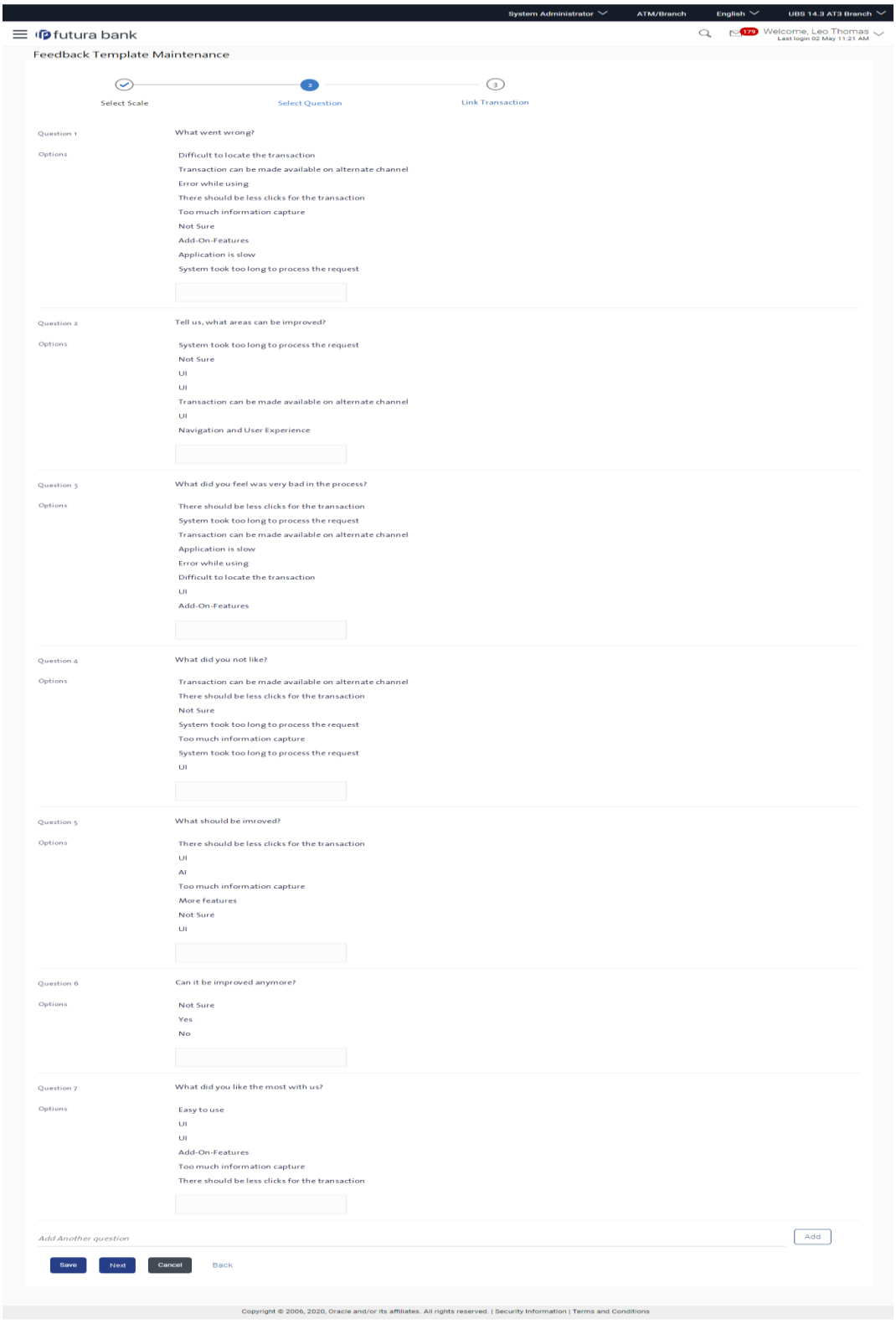
Feedback Template - Edit



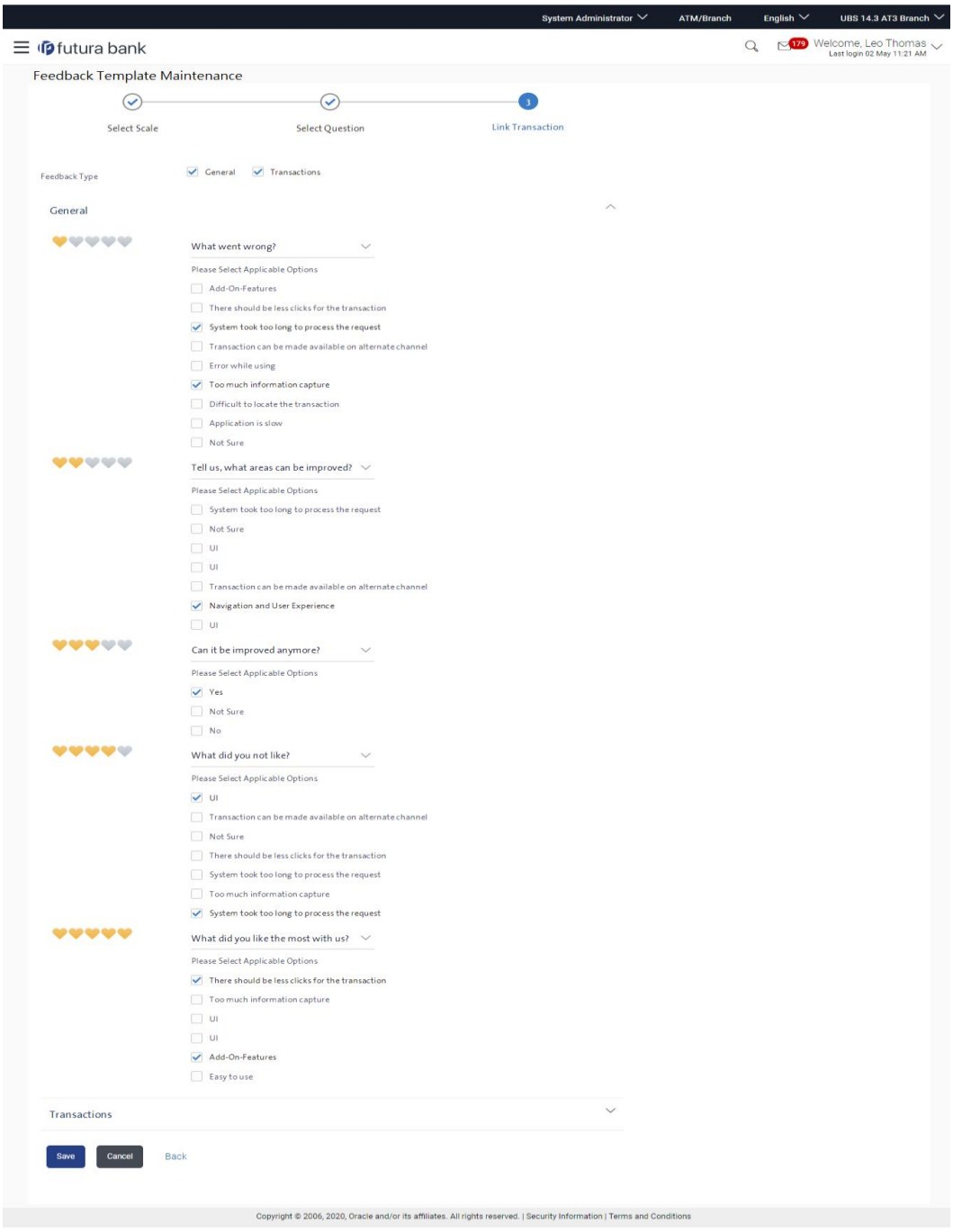
Select Scale - Edit



Select Question – Edit



Link Transaction - Edit



15. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to go to previous screen.
16. The success message with reference number appears.
    Click **OK** to complete the transaction.

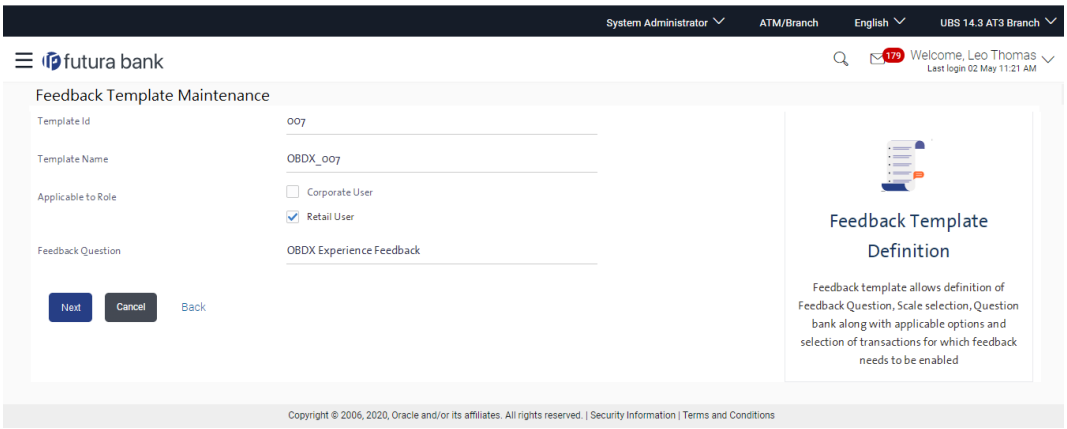
21.1.3 Feedback Template Maintenance - Create

Using this option, the administrator can create feedback template for a specific user type i.e. retail / corporate by defining the details i.e. the feedback question, selecting the rating scale, addition of new questions along with options, select transactions for which the feedback capture needs to be enabled.

To create feedback template:

1. Navigate to the **Feedback Template Maintenance** screen and click **Create**. The **Feedback Template Maintenance - Create** screen appears.
2. In the **Template ID** field, enter the template ID.
3. In the **Template Name** field, enter the name of the template.
4. Select the role(s) for which the feedback template is applicable by selecting check box in the **Applicable to Role** field.
5. In the **Feedback Question** field, enter the name of the feedback question.

Feedback Template Maintenance - Create



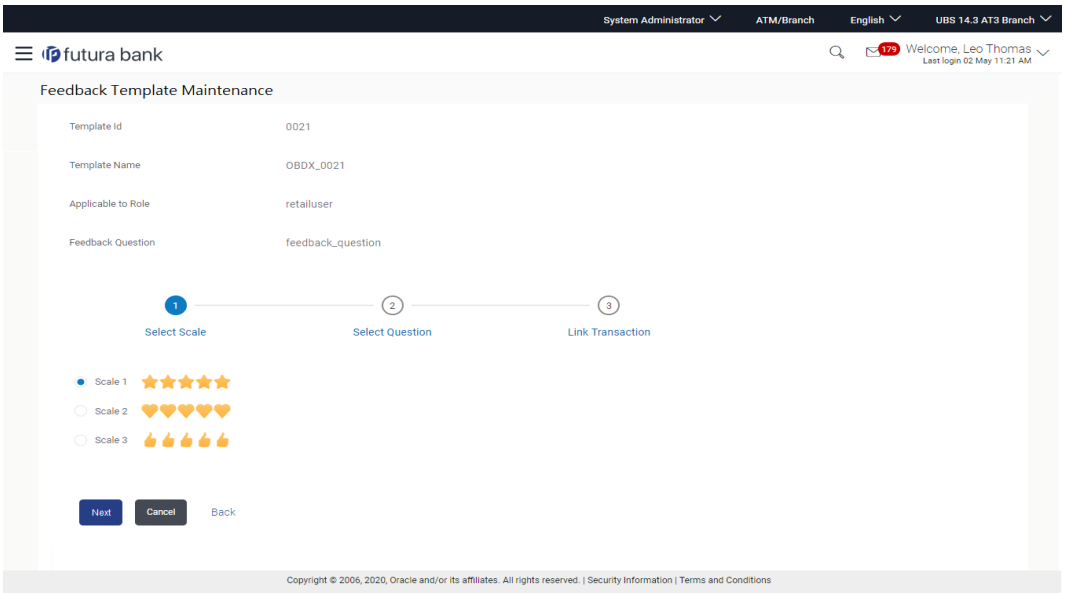
Field Description

Field Name	Description
Template ID	Enter the template ID.

Field Name	Description
Template Name	Enter the template name for the template being created.
Applicable To Role	Select the role(s) for which the template will be applicable. You can select multiple roles and the system will resolve the template based on the role of the user when the user wishes to capture feedback.
Feedback Question	Define the feedback question. This is the question that will be asked to the user as part of feedback capture on which he/she can rate on the rating scale.

6. Click **Next**. The select scale screen section in the feedback template maintenance screen is displayed.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Feedback Template Maintenance - Select Scale

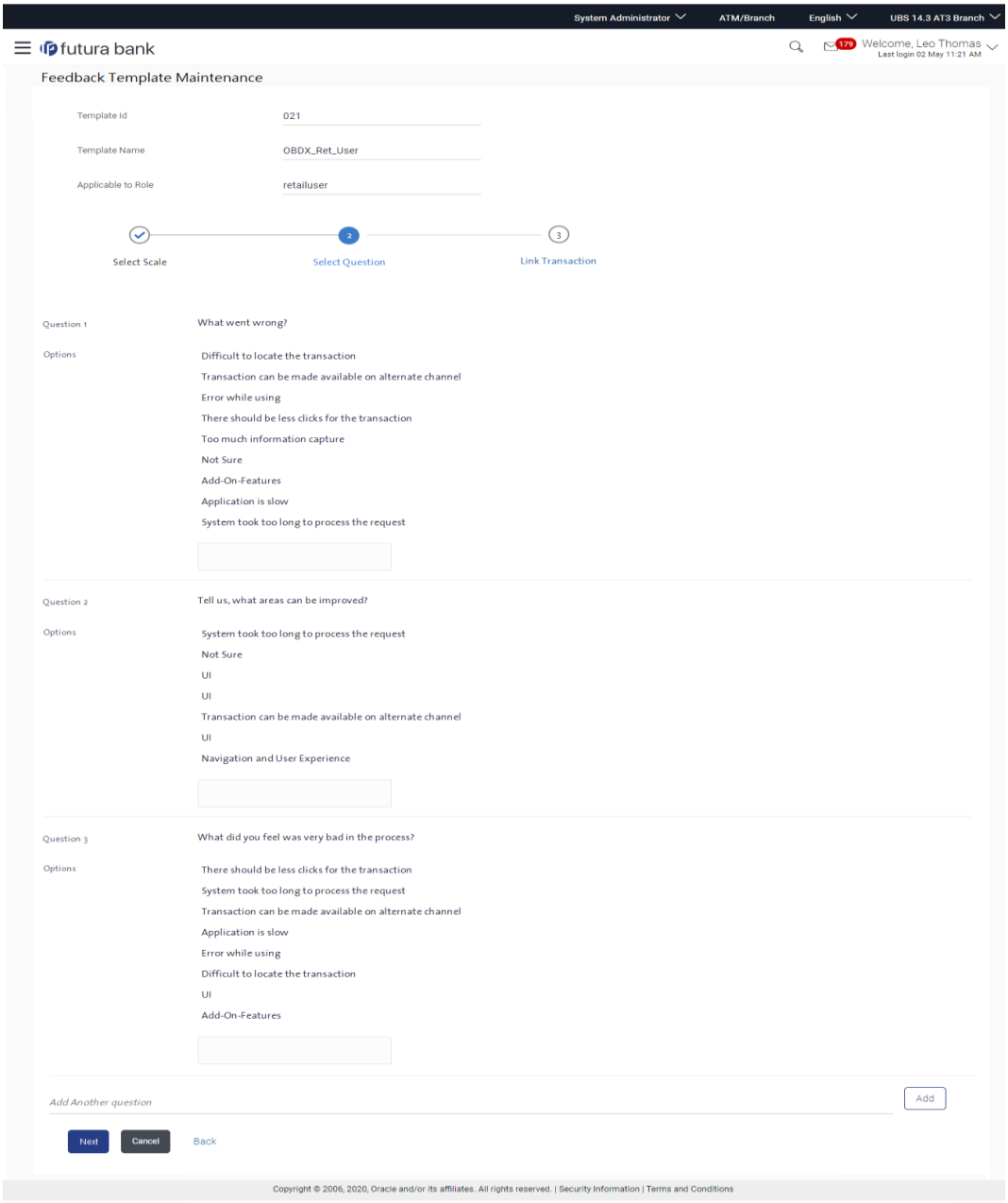


Field Description

Field Name	Description
Select Scale	Select the required scale. The scale will be available for the user to rate as part of feedback capture.

7. In the **Select Scale** field, select the appropriate option.
8. Click **Next**. The select question section as part of **Feedback Template Maintenance** screen is displayed.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Feedback Template Maintenance - Select Question



Field Description

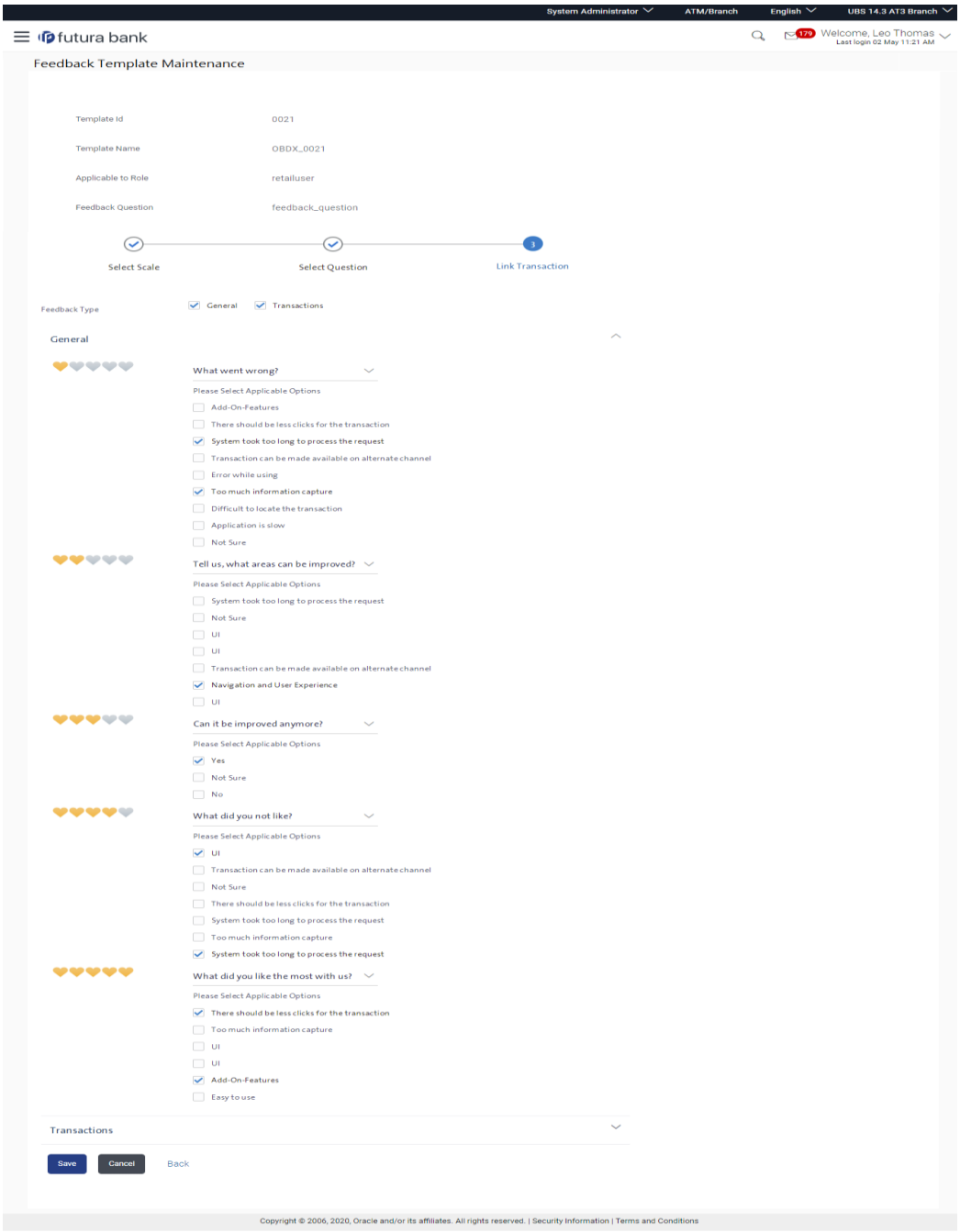
Field Name	Description
Select Question	
Question	Displays the default questions as defined in the system. The user can add new questions as part of the template definition. The default questions as well as the newly added questions will be associated to the scale weight of the rating scale.
Options	Displays the default options as defined in the system. The user can add new options as part of the template definition. The newly added options can be associated to the existing default questions as well as newly added questions.

9. Click in the **Options** field to add more options to the existing questions.
10. To add a new question, type the question in the text area in 'Add another question' and click the **Add button**.
11. Once the question is added, click in the **Options** field to add answers to the newly added questions.

Note: Click to delete the newly added question.

12. Click **Next**. The **Feedback Template Maintenance** screen is displayed.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.

Feedback Template Maintenance - Link Transaction



Field Description

Field Name	Description
Link Transactions	

Field Name	Description
Feedback Type	Indicates whether feedback type is general or is specific to transaction. The options are: • General: This is very generic in nature and not feedback specific to a transaction. The template defined will be applicable when the user wishes to leave feedback generally through the menu option. • Transactions: This is in case wherein administrator wants to define the template very specific to a set of transaction or a set of transactions.

13. Select the applicable feedback type i.e. general or transactions or both
14. If you select **General** option, there will be a panel available to define questions along with options against each of the scale weights of the rating scale. It is not mandatory to assign a question to each scale weight.
15. If you select **Transaction** option, there will be a panel available to select the transactions in the **'Select transaction'** field and also define questions along with options against each of the scale weights of the rating scale. It is not mandatory to assign a question to each scale weight.
16. Click **Save** to save the template information.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.
17. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to go to previous screen.

FAQ

1. **Can I define multiple feedback questions as part of the template definition?**

   No. Only one feedback question can be defined as part of the template and this will be asked to the business user on which he/she will rate. The same question will be applicable to General feedback and for transactions.

2. **What is the relevance of the questions and option set defined as part of select question section?**

   The questions and options defined as part of the select question section are used for association to the scale weights if required which will be asked to the user on he/she selecting the weight on the rating scale as part of actual feedback capture.

3. **Can I have separate questions associated at scale weight level for different transactions?**

   Yes, you will need to select and group transactions for which you wish to have common questions and options at scale weight level. Click on Add Another Transaction to add transactions that require different set of questions and options at scale weight level.

4. **Can I remove the questions associated at scale weight level as part of edit?**

   No. Currently questions once defined can't be removed.

5. **Can the same feedback template be applicable to multiple roles?**

   Yes, provided multiple roles have been selected in the 'Applicable to Role' field.

21.2 Feedback Analytics

Feedback Analytics gives the bank a quick analysis of the feedback information collected from the customers. The analytics covers information about the average of feedback ratings that transactions have got, trends in how the average ratings have changed the top and bottom transactions in terms of ratings etc. The analytics helps banks in quickly identifying the pain points in customer journeys and points out the specific areas for improvement and action.

Using this option, the System Administrator can analyse the feedback given by users.

The following information will be available to the administrator as part of analytics:

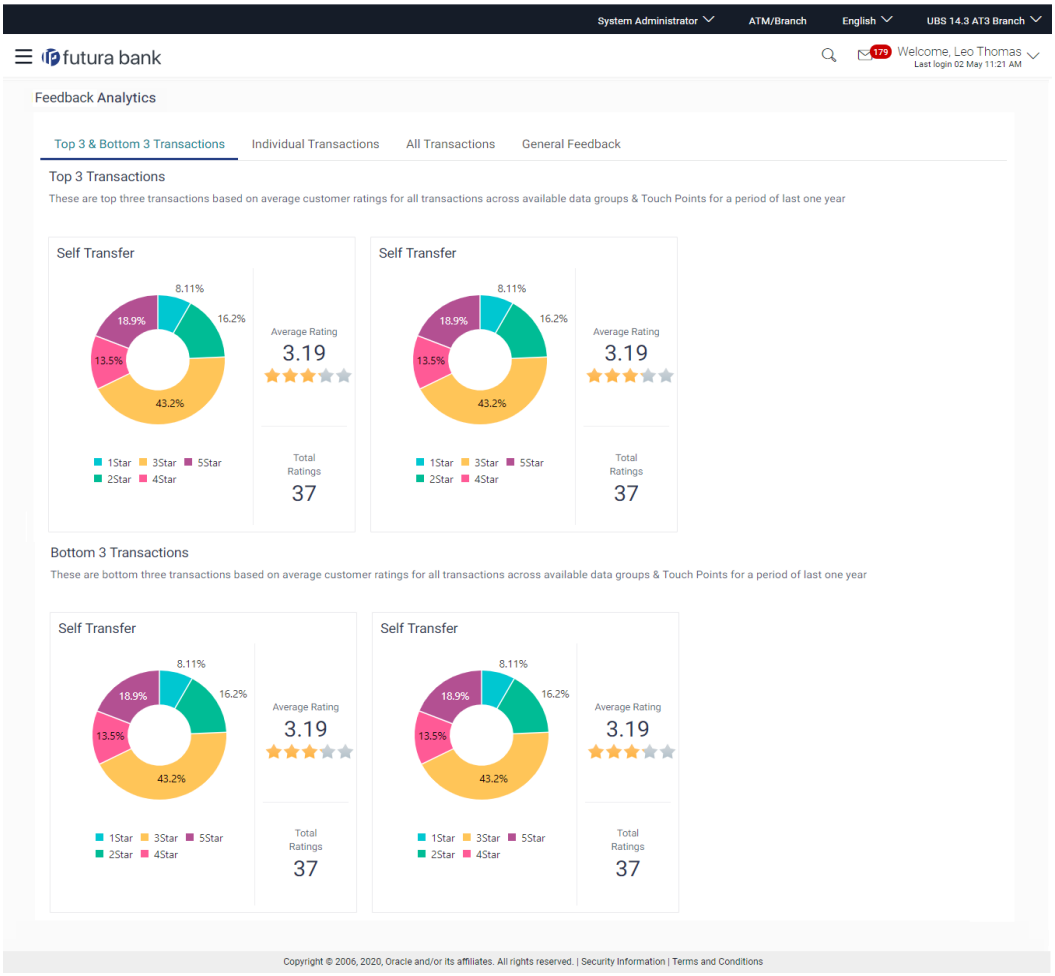
- Top three and bottom three transactions: Shows the top three and bottom three transactions based on user given rating
- Individual Transactions: Shows the user given ratings, distribution of the ratings given, the answer options chosen for the associated question & change of ratings over three time periods for an individual transaction
- All Transactions : Shows the user given ratings, distribution of the ratings given, and change of ratings over three time periods
- General Feedback: Shows the user's general feedback i.e. Average rating for the selected time period, Rating over time (last month, last quarter, last year), Recent comments by user grouped based on ratings, and the Customer response for the question associated with each rating

How to reach here:

System Administrator Dashboard > Controls & Monitoring > Feedback Analytics
OR
System / Bank Administrator Dashboard > Toggle Menu > Menu > Controls & Monitoring > Feedback Analytics

21.2.1 Top Three and Bottom Three Transactions

Top three and bottom three transactions



Field Description

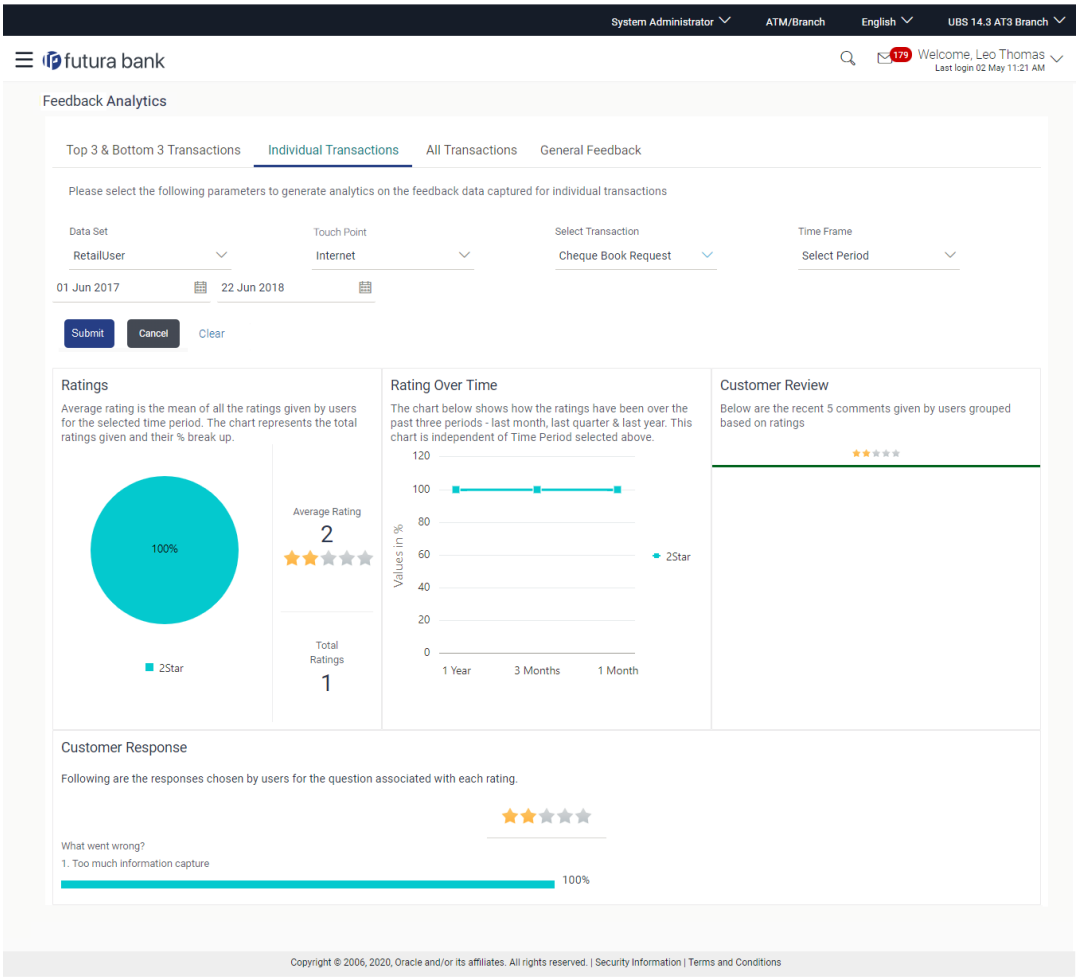
Field Name	Description
Top / Bottom 3 Transactions	Displays the top / bottom three transactions in graphical format. It also displays the ratings given by the user to that particular transaction.

21.2.2 Individual Transactions

To view individual transactions:

1. From the **Data Set** list, select the user for which the transaction is to be searched.
2. From the **Touch Point** list, select the banking channel.
3. From the **Select Transaction** list, select the transaction name for which the feedback is to be searched.
4. From the **Time Frame** list, select the duration in number of months / years.
5. Click **Submit**. The search results are displayed.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search criteria.

Individual Transactions



Field Description

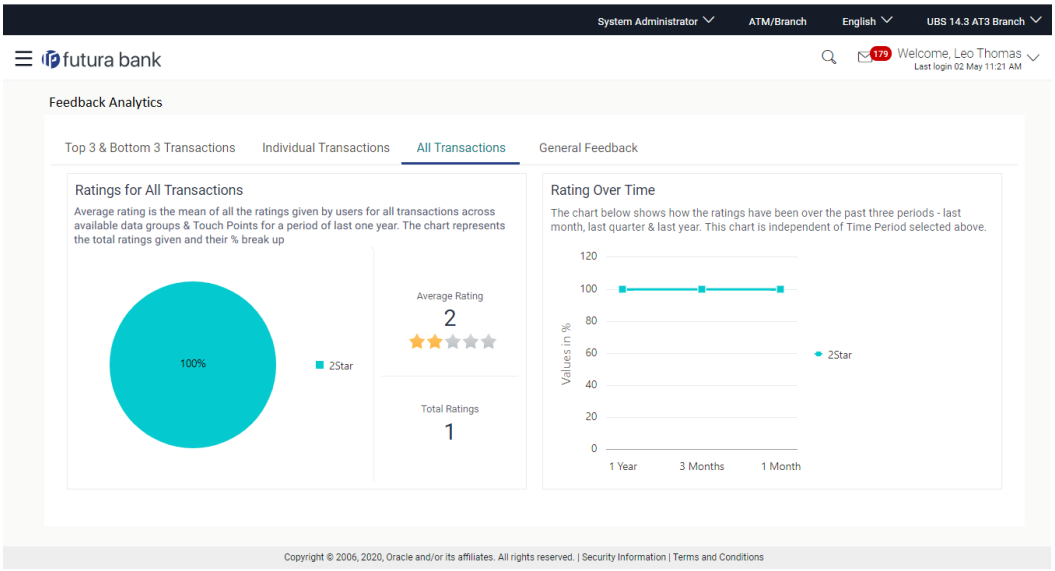
Field Name	Description
Data Set	Select the type of the user from the list. The options are: • Administrator • Corporate User • Retail User
Touch Point	Select the banking touch point from the list. The options are: • Mobile Application • Internet • Mobile (Responsive) • Wearables • Missed Call Banking • SMS Banking • Siri / Chatbot • Snapshot
Select Transaction	Select the transaction from the list for which you wish to analyze the feedback.
Time Frame	Select the time period for which you wish analyze the feedback. You can search the feedback on the basis of time range, by entering the **From Date** and **To Date**. The **From Date** and **To Date** fields are displayed, if you select **Select Period** option from the **Time Frame** field.

21.2.3 All Transactions

To view all transactions:

1. From the **Data Set** list, select the user for which the transaction is to be searched.
2. From the **Touch Point** list, select the banking channel.
3. From the **Select Transaction** list, select the transaction name for which the feedback is to be searched.
4. From the **Time Frame** list, select the duration in number of months / years.
5. Click **Submit**. The search results are displayed.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search criteria

All Transactions



Field Description

Field Name	Description
All Transactions	Displays the feedback for all transactions and for a period. The feedback is segregated in: • Ratings for All Transactions: It is a rating given by the users for all transactions across available data groups and touch point for last one year.

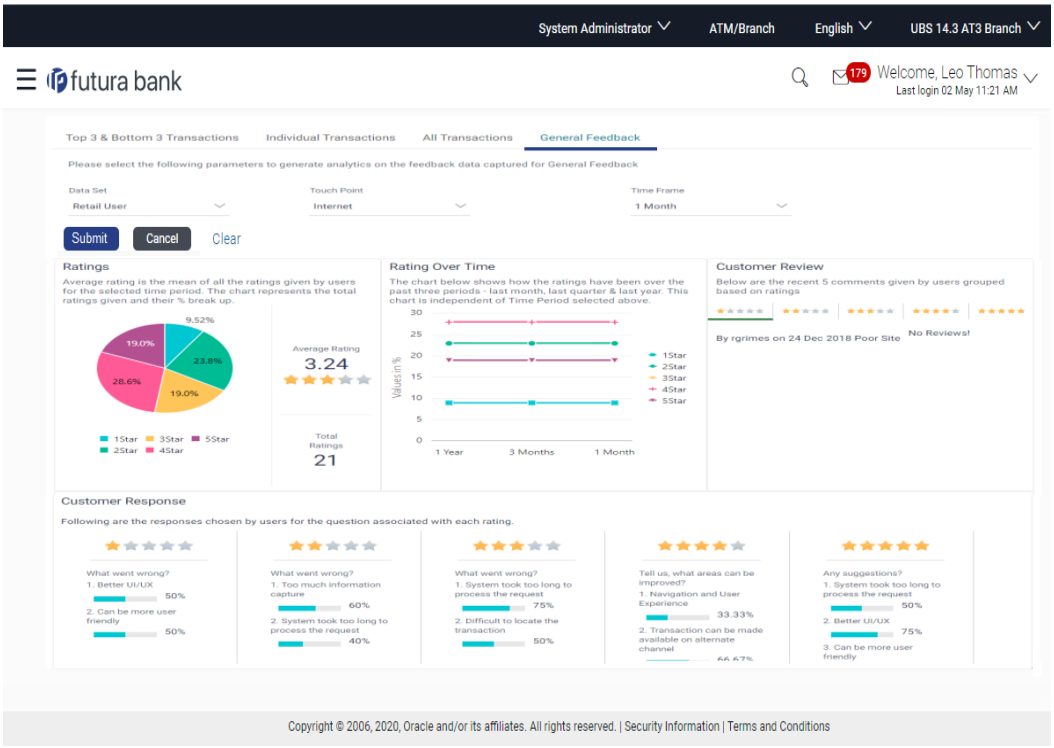
Field Name	Description
	• Rating Over Time: It is a rating given for a period of time, for example, one month, three month and one year.

21.2.4 General Feedback

To view general feedback:

1. From the **Data Set** list, select the user type for which general feedback is to be viewed.
2. From the **Touch Point** list, select the banking channel for which feedback information needs to be viewed.
3. From the **Time Frame** list, select the duration for which the feedback information needs to be viewed.
4. Click **Submit**. The results are displayed based on the search criteria input.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search criteria

General Feedback



Field Description

Field Name	Description
Data Set	Select the type of the user from the list. The options are: • Corporate User • Retail User
Touch Point	Select the touch point from the list. The options are: • Internet • Mobile (Responsive) • Mobile Application
Time Frame	Select the time period for which you wish analyze the feedback from the customer. You can search the feedback on the basis of time range, by entering the **From Date** and **To Date**. The **From Date** and **To Date** fields are displayed, if you select **Select Period** option from the **Time Frame** field.
Search Result	
General Feedback	Displays the general feedback details for and the selected search parameters. • Ratings: It displays the percentage of ratings for each rating given by the users as part of general feedback. It also displays the average rating value and also displays the total no. of ratings. • Rating Over Time: It displays the general feedback ratings given over a time period i.e. last month, last quarter, last year. • Customer Review: It displays the recent 5 comments provided by users and grouped based on ratings. • Customer Response: It displays responses chosen by users for the question associated with each rating

22. SMS Banking

SMS and Missed call banking gives business user the control to manage his/her account whenever and wherever needed by sending a SMS or by giving a missed call on a designated number.

Business user just needs to register his/her mobile number with the bank and explicitly opt for SMS/Missed Call banking services to access the required information.

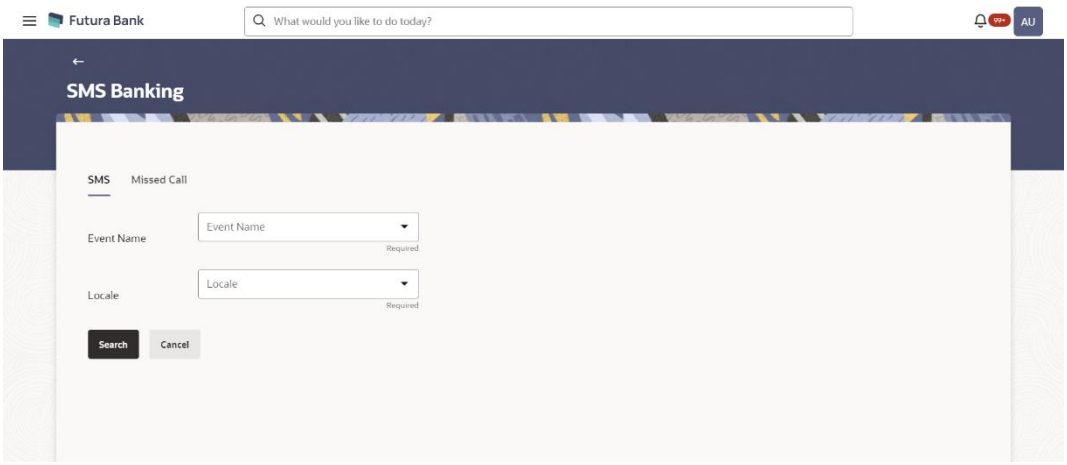
Using this option, the system administrator can maintain the following templates

- **SMS Banking:** The template for an event and locale combination can be created by defining the input keyword, data attributes, whether PIN required and response message.
- **Missed Call Banking:** The template for an event and locale combination can be created by defining the contact number on which the customer would need to give a missed call and response message.

How to reach here:

System Administrator Dashboard > Templates > SMS and Missed Call Banking > SMS
OR
System / Bank Administrator Dashboard > Toggle Menu > Menu > Templates > SMS and Missed Call Banking

SMS Banking - Search



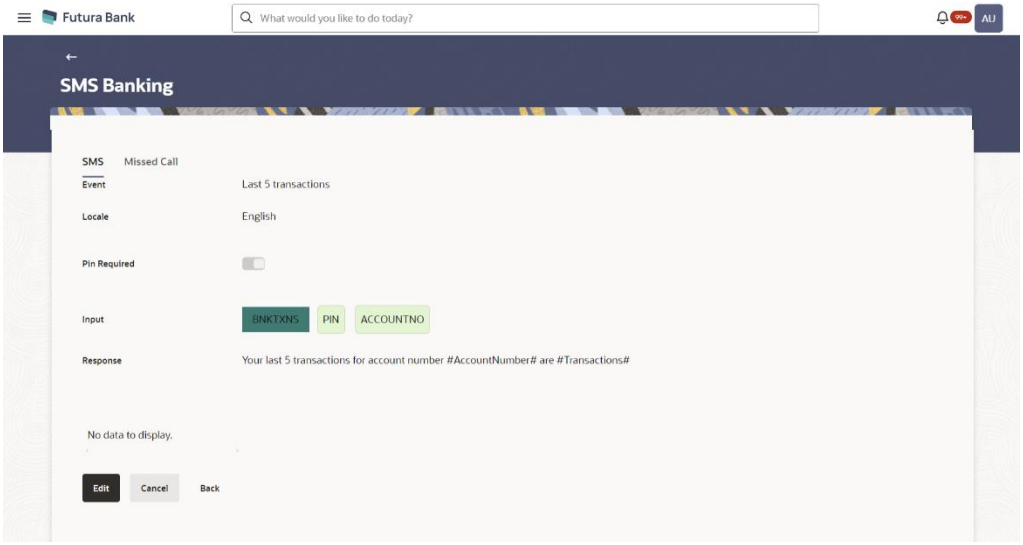
To search SMS template:

1. From the **Event Name** list, select the appropriate event.
2. From the **Locale** list, select the language.
3. Click **Search**. The View screen appears, depending on the search criteria.

   OR

   Click **Cancel** to cancel the transaction.

SMS Banking - View



Field Description

Field Name	Description
Event Name	Select the event name.
Locale	Select the locale of the template. Currently only ‘English’ is supported
Event Name	Displays the event name as selected on the search page for which the template details are to be viewed.
Locale	Displays the language in which the SMS template is defined i.e. input syntax as well as the response message
Pin Required	Indicates whether PIN is required while requesting information from the bank.
Input	Displays the input syntax containing the keyword, data attribute(s) and PIN (if required) for the selected event and locale combination The format in which the user needs to send the text message with the required attribute(s) to receive appropriate information.

Field Name	Description
	For example: If the account holder wishes to receive account balance information from the bank and the template is defined as MBAL <PIN> <AccountNumber>, user's PIN is defined as 5678, and account number is AT30012100012, then user will need to send SMS as MBAL 5678 AT30012100012.
Response	Displays the response message along with the data attributes as defined for the event and locale combination. It is the response message that the account holder would be receiving on sending a SMS for a specific inquiry or transaction.
Data Attributes	Displays the data attributes used as part of response message for the respective event.

4. Click **Edit** to if you want to edit the SMS template.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

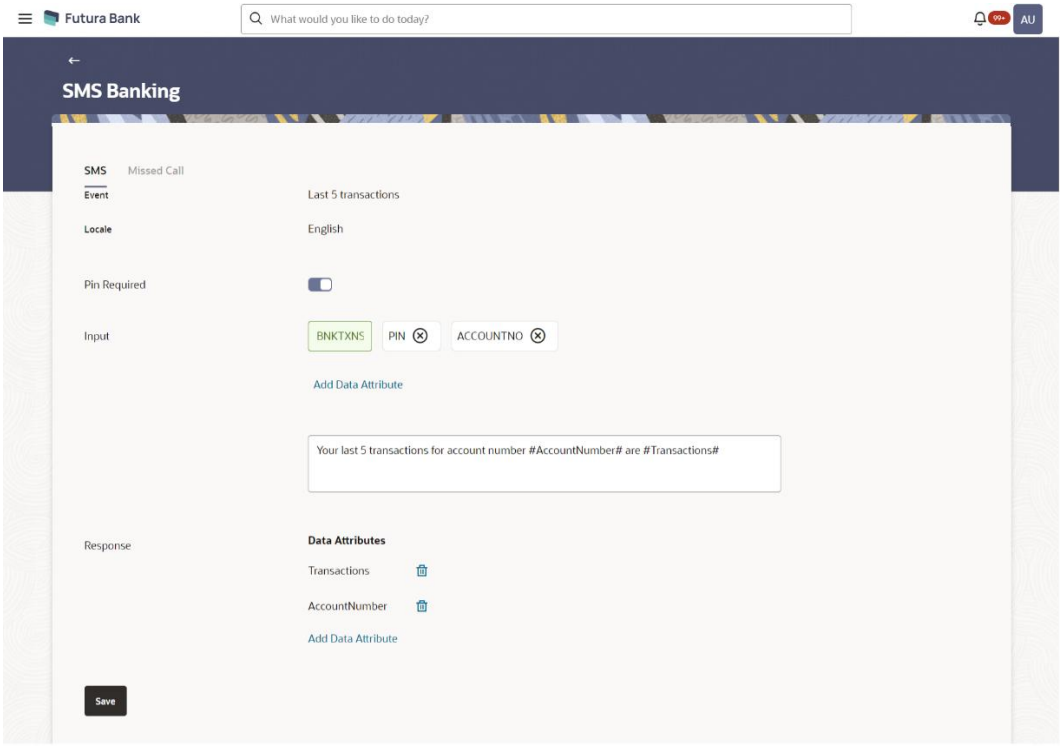
22.1 SMS Banking - Edit

Using this option, System Administrator can modify the SMS Banking template defined for an event and locale combination.

To edit or update a SMS template:

1. Select the Event and Locale and click **Search**. You will be navigated to the SMS Banking Template in View mode.
2. Click **Edit** to modify the details. The **SMS Banking- Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

SMS Banking - Edit



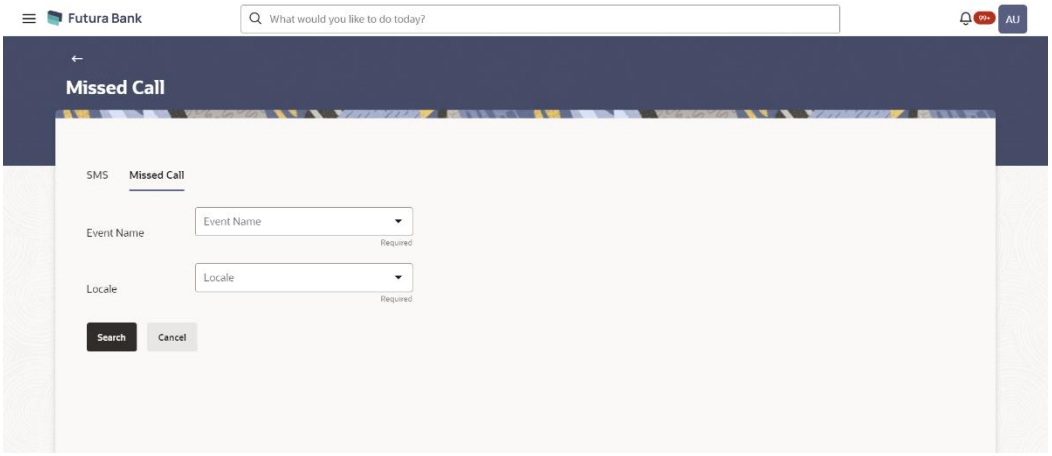
3. As part of edit, you can modify the keyword defined for the event, include new data attributes in the input syntax or remove existing data attributes, modify the response message and also include new data attributes as part of response message.
4. Click **Save** to update the changes.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction.
5. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Back** to go to previous screen.
   OR
   Click **Cancel** to cancel the transaction.
6. The success message about modification appears.
   Click **OK** to complete the transaction.

22.2 Missed Call Banking - Search

How to reach here:

Administrator Dashboard > Templates > SMS and Missed Call Banking > Missed Call

Missed Call Banking - Search



Missed Call Banking - Search

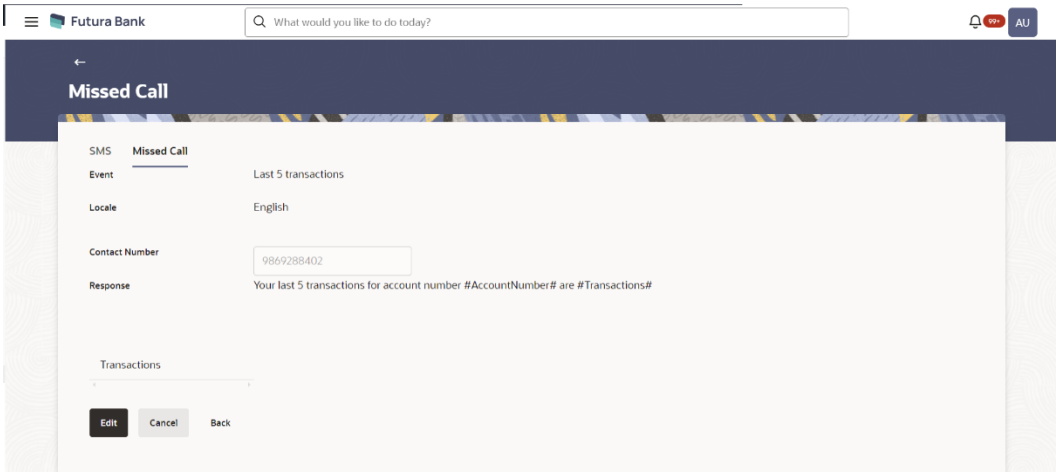
To search Missed Call Banking template:

1. From the **Event Name** list, select the appropriate event.
2. From the **Locale** list, select the language.
3. Click **Search**. The View screen appears, depending on the search criteria.

   OR

   Click **Cancel** to cancel the transaction

Missed Call Banking - View



Field Description

Field Name	Description
Event Name	Select the event name from the list.
Locale	Select the locale of the template. Currently only 'English' is supported.
Event Name	Displays the event name as selected on the search page for which the template details are to be viewed
Locale	Displays the locale as selected on the search page for which the template details are to be viewed It is the language in which the information is communicated to the account holder on request.
Contact Number	Displays the contact number defined for the selected event and locale combination on which the user needs to give a missed call to get the required information.
Response	Displays the response message as defined for the event and locale combination with the required data attributes. It is the response message that the account holder would be receiving when he gives a missed call on a specific contact number
Data Attributes	Data attributes that are used as part of response message for the respective event.

4. Click **Edit** to if you want to edit the missed call template.
   OR

Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate to the previous screen.

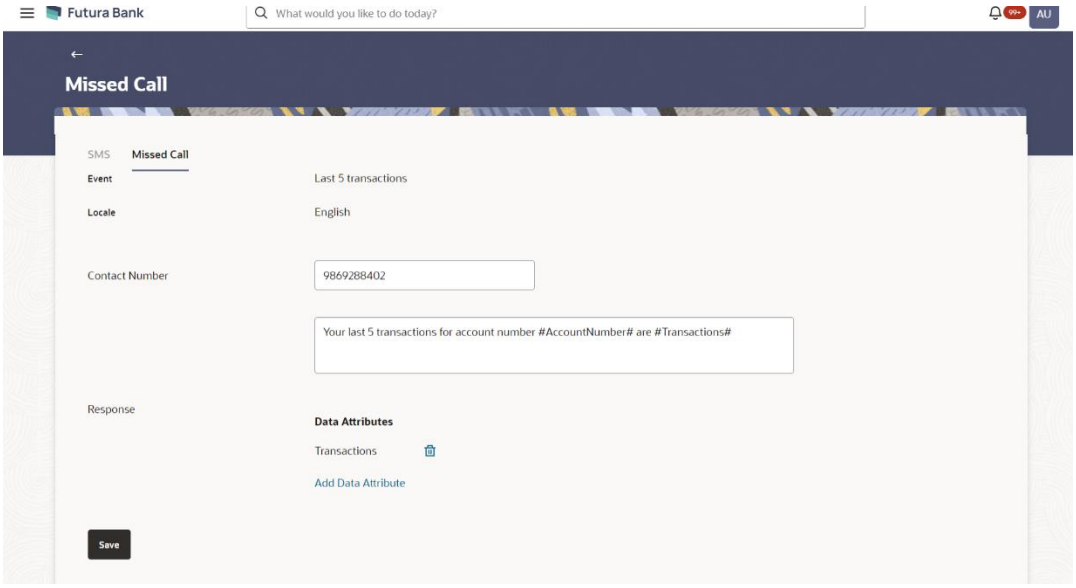
22.3 Missed Call Banking - Edit

Using this option, System Administrator can modify the Missed Call Banking template defined for an event and locale combination.

To edit or update a missed call template:

1. Select the Event and Locale from the list and click **Search**. You will be navigated to the **Missed Call Banking** template in View mode.
2. Click **Edit** to modify the details. The **Missed Call Banking- Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Missed Call Banking - Edit



3. As part of edit, you can modify the contact number as well as the response message
4. Edit the required details.
5. Click **Save** to update the changes.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Back** to go to previous screen.

OR
Click **Cancel** to cancel the transaction.

7. The success message about modification appears.
   Click **OK** to complete the transaction.

FAQ

1. **How can the business user register for SMS Banking?**

   User can send a SMS with the required keywords and data attributes defined by the bank to a specified contact number. User needs to send the SMS from his/her registered mobile number with the bank. Alternatively he/she can login to Internet Banking and register for SMS Banking.

2. **Is it mandatory to have a PIN in each of the request for SMS Banking?**

   It will depend on the template defined for event and locale combination. If PIN is required, then user needs to define the PIN as part of registration process and subsequently send that as part of the request.

3. **Does the user need to specify an account number as part of the request while sending SMS?**

   No, it is not necessary. If the user does not specify the account number, system will return response for the primary account number if defined.

4. **For which account does system return the response in case of Missed Call Banking?**

   System will always return the response for the primary account number (if defined) on receipt of request through missed call banking

5. **User is unable to receive information and getting an error, how can he/she find the correct keyword?**

   User might be getting an error due to keyword and/or account number not being valid or the required data attributes not present. He/she can find the keywords by sending a help message and system will return the set of business functions supported through SMS Banking along with keywords for each of the transactions.

6. **Should the user be on-boarded on channel platform for him/her to access SMS Banking?**

   Yes, the user needs to be on-boarded on OBDX with SMS Banking as a touch point enabled to access SMS Banking.

23. System Rules

System rules are defined to set different parameters for each enterprise role (User Type- Retail, Corporate and Administrator). Various parameters that can be set for each enterprise role are Party Mapping required Limits check, Party Preferences check, Account Transaction Mapping and Approvals check, Group Corporate Check. Enabling these parameters at enterprise role, enforces the system to check if respective maintenances are available for users associated with those enterprise roles.

E.g. if Approval check flag is enabled for 'Corporate User' type of enterprise role; then transactions initiated by corporate type of users will follow the approval maintenance for a party mapped to user and vice versa.

The flag 'Group Corporate' is applicable only for 'Corporate User' type of enterprise role. This flag in System Rules screen defines the mode of corporate onboarding.

If **Group Corporate** flag is set 'ON' then Bank administration will be able to onboard Group Corporate. The **Group Corporate** flag is enabled by default and always "ON".

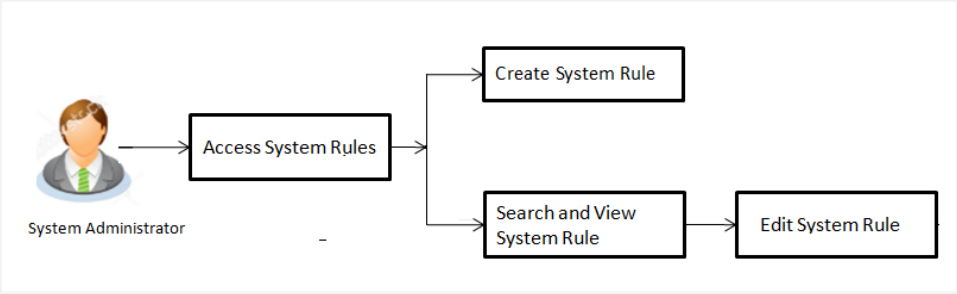
When in the **Enterprise Role** field user type is selected as **Corporate User**, then the **Group Corporate** flag will get displayed in non-editable mode.

This screen allows the System Administrator to search and view existing system rules, and create new system rule.

Pre-Requisites

- Transaction access is provided to System Administrator.
- Approval rule set up for System Administrator to perform the actions.
- Enterprise roles are maintained in application.
- Touch point groups are maintained, if required.
- Limit packages are maintained.

Workflow



Features Supported In Application

This option allows the System Administrator to:

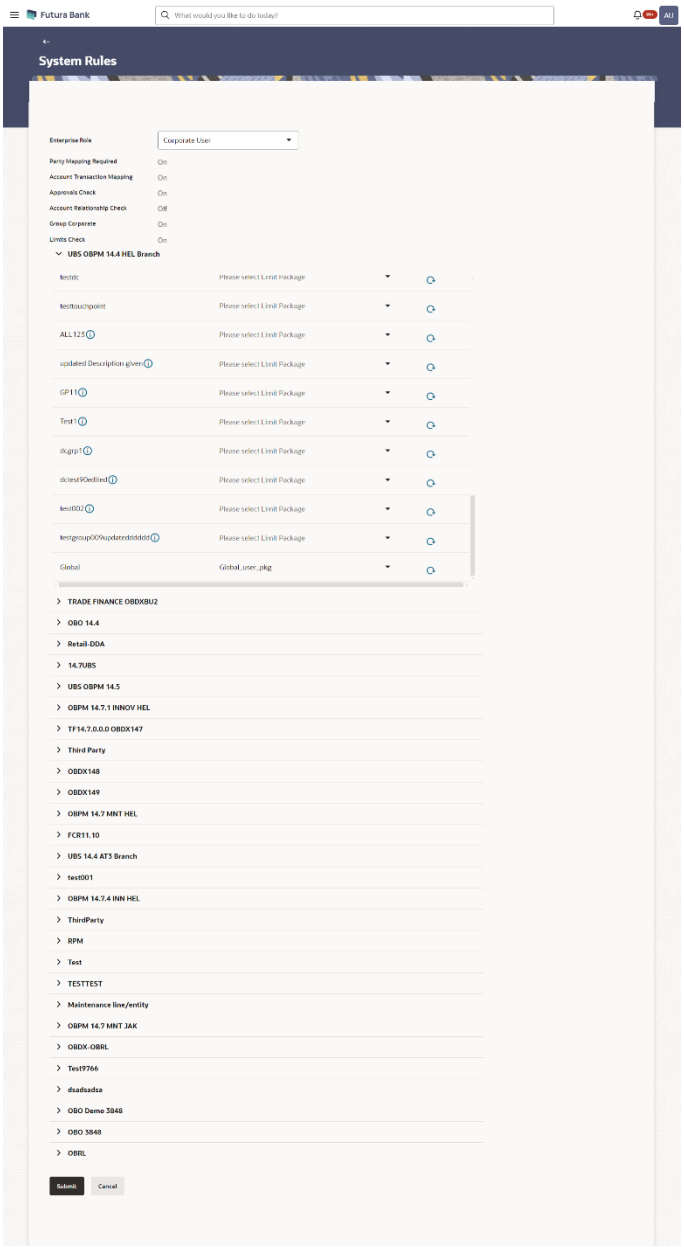
- Maintain system rules

- View system rules
- Edit system rules

How to reach here:

System Administrator Dashboard > Configuration > System Rules
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Configuration > System Rules

System Rules



Field Description

Field Name	Description
Enterprise Role	Name of enterprise roles set in application. The options can be: • Corporate User • Administrator • Retail User On selecting an application role, system rules maintained if any, are shown in editable form.
Party Mapping Required	Party mapping check is required for a particular enterprise role or not.
Party Preferences Check	Party preferences check is required or not.
Account Transaction Mapping	Account transaction mapping check is required or not.
Approvals Check	Approvals check is required or not.
Account Relationship Check	Account Relationship check is required or not. Note: The Account relationship check has to be disabled for the corporate user.
Group Corporate Check	Group Corporate onboarding is required for corporate or not**.** Note: 1) The **Group Corporate** flag is enabled by default and always "ON". When in the **Enterprise Role** field user type is selected as **Corporate User**, then the **Group Corporate** flag will get displayed in non-editable mode. 2) Group Corporate flag = 'On', then Bank administration will be able to onboard Group Corporate.
Limits Check	Limits check is required or not.

Field Name	Description
Limits - Entity Level Configuration	
If limit check is required, assign a limit package.	
In case of multi entity set up, limit packages needs to be mapped at each entity level.	
Name of the entity	Name of entity under which limit packages are to be mapped is shown in the header.
Touch Points/ Group	Name of touch points/ groups under a specific entity to whom the limit packages are to be mapped. Also an option is provided to map the limit package at Global level (a group created with all internal and external touch points)
Package	List of the packages which are to be mapped to a touch points/ groups. Only limit packages maintained for the selected touch point will get listed here.

To set the system rules:

1. From the **Enterprise Role** list, select the appropriate option.
2. In the **Party Mapping Required** field, select the appropriate option.
3. In the **Party Preferences Check** field, select the appropriate option.
4. In the **Account Transaction Mapping Check** field, select the appropriate option.
5. In the **Approvals Chec**k field, select the appropriate option.
6. In the **Account Relationship Check** field, select the appropriate option.
7. In the **Group Corporate Check** field, select the appropriate option.
8. In the **Limits Check** field, select the appropriate option.

    a. Click of desired entity to whom limit package to be mapped. Displays the list of touch points/ groups to map limit package.

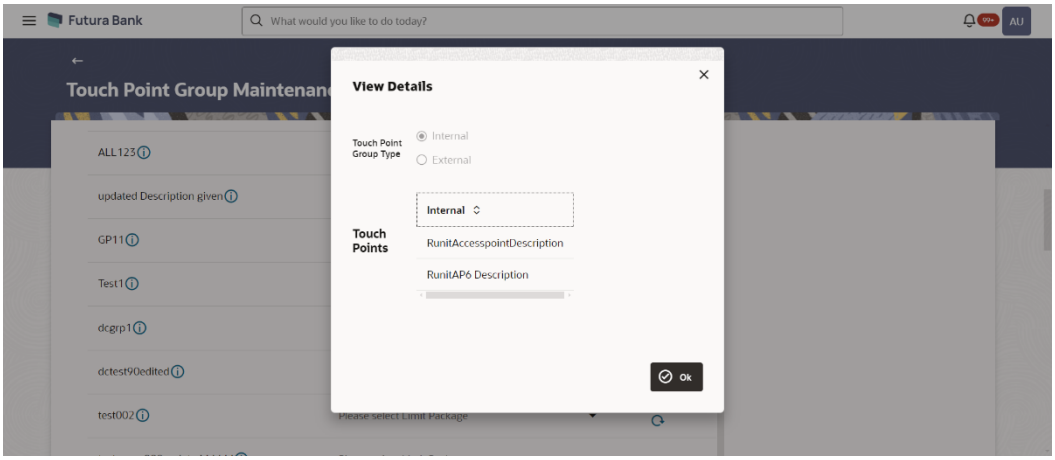
    b. From the **Package** list, select the appropriate option.

Note: Click to refresh the option.

    c. Repeat steps a to b of step 8 for all touch points/ groups.

        i. Click to view the details of touch points group. The **View Details -Touch Point Group** popup window appears.

View Details -Touch Point Group



Field Description

Field Name	Description
Group Code	Group code defined for a touch point group.
Group Description	Group description defined for a touch point groups.
Touch Point Group Type	Type of touch point i.e. whether touch point is of type internal or external.
Touch Points	List of the internal or external touch points.

9. Click **Submit** to save system rules.
   OR
   Click **Cancel** to cancel the transaction.
   The success message appears.
10. The **System Rules - Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Back** to make the changes if any.
    OR
    Click **Cancel** to cancel the transaction and navigate back to ‘Dashboard’.
11. The success message of System Rules maintenance appears along with the transaction reference number. Click **OK** to complete the transaction.

FAQ

1. **Who can create-edit this maintenance?**

   System Administrator can create and edit this maintenance.

2. **How can I find out what checks are granted to a particular role and can I change it?**

   You can select a role and view the checks mapped to the role, you can also edit the type of checks.

3. **How can I group the touch points?**

   A separate menu option ‘Touch Point Group Maintenance’ is available to the system administrator user to maintain the groups. Groups maintained under specific entity are shown on the System Rules screen against which a consolidated limit package can be assigned.

4. **Is it mandatory to map packages for all the touch points and groups available under each entity?**

   Mapping the limit packages for each touch point and for all groups available under each entity is not mandatory. But it is mandatory to map a limit package at Global level for each entity.

24. Timer Maintenance

This feature allows users to schedule a specific event to run at fixed intervals. The Bank Admin can set the timer for the event and is also allowed to view and update the event details as needed.

Timer Maintenance feature allows the system administrator to view, update, enable or disable the existing timers, where they can reschedule or enable / disable the existing timers it will reflect with immediate action on the fly without need for restarting system, which mean they will get triggered with next execution date as per the updated schedule.

Note: On update or enable/disable Timer it will reflect the schedulers of all active entities exists within OBDX.

Pre-requisites

- Transaction access is provided to System Administrator.
- Approval rule set up for System Administrator to perform the actions.
- Default Timers comes with Base product and customized Timers which are defined within the OBDX can be modified.

Features Supported In Application

This option allows the System Administrator to:

- Search Timer
- View Details of Timer and description of Cron Expression (represents run schedule in human readable description form)
- Edit Timer schedule
- Enable / Disable existing Timer

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Configuration > Timer Maintenance
OR
Search bar > Configuration - Timer Maintenance

24.1 View Timer

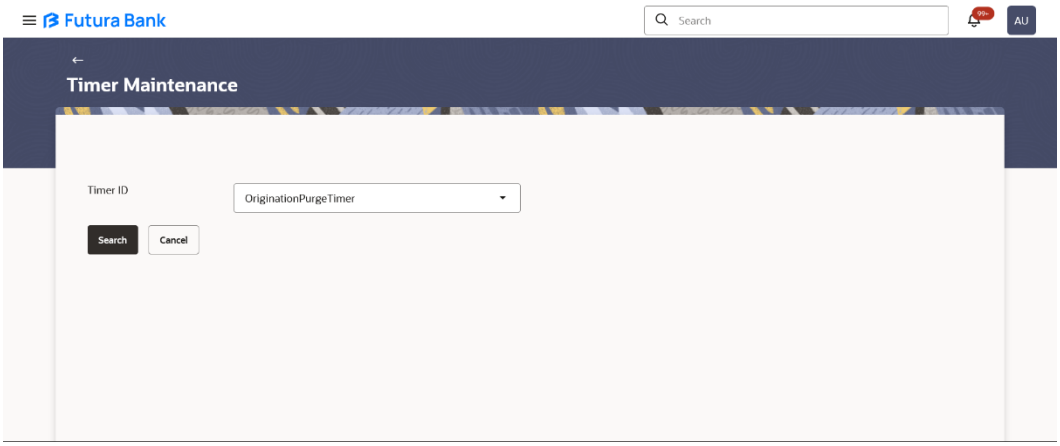
The option shows list of all Timers within OBDX system and allow to search required timer to do maintenance on it. It will display the details of Timer on which we are allowed to perform maintenance.

Note: Description is not stored in System, it is the description explaining the Cron Expression indicating the running schedule of the underlying Timer.

To search and view the timer :

1. Navigate to the **Timer Maintenance** screen.

Timer Maintenance - Search

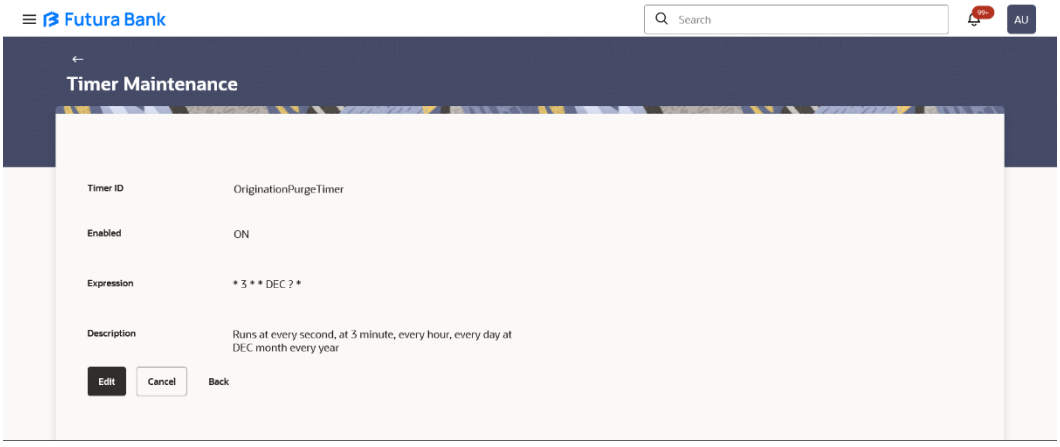


Field Description

Field Name	Description
Timer ID	Name of event for whose timer details to be searched.

2. From the **Timer ID** list, select the event whose timer details to be searched.
3. Click **Search**. It displays the details of the selected Timer and show the details in **Timer Details** Screen.

Timer Maintenance – Timer Details (View)



Field Description

Field Name	Description
Timer ID	Name of event for which timer is to be set.
Enabled	Displays the whether the timer is active or not.
Expression	Displays the expression set for the selected event. The format to set the timer is <**Seconds> <Minutes> <Hours> <Day of Month Month> <Day Of Week> <Year>**. Note: 1) Click the ⓘ icon to view the expression format. 2) Click the Validate Expression to execute the expression and validate it.
Description	Displays the expression details.

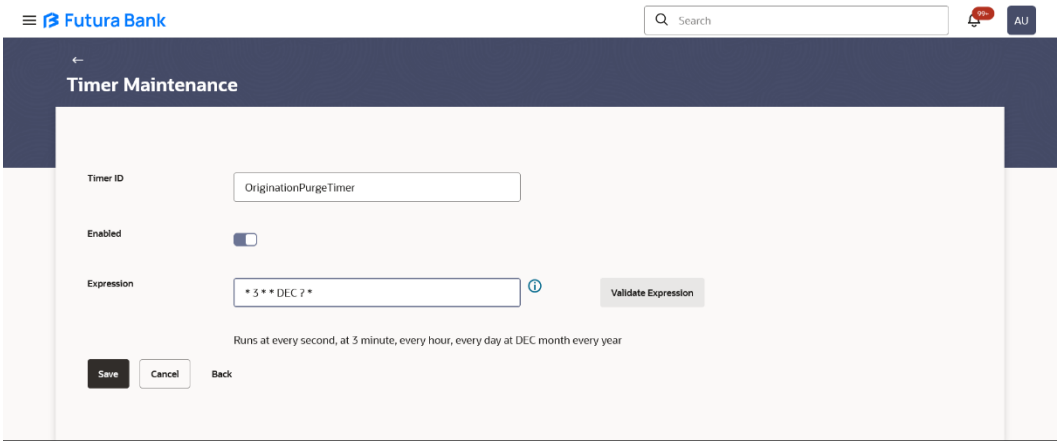
24.2 Update Timer

Using this option administrator can modify the execution schedule of the underlying Timer. Also, administrator can enable disable the execution of the Timer within System.

To update the timer details :

1. Navigate to the **Timer Maintenance** screen.
2. From the **Timer ID** list, select the event whose timer is to be set.
3. Click **Search**. The details of selected event appears.
4. Click **Edit** to modify the execution schedule of the underlying Timer. The Timer Details appears in editable mode.
5. Update the Expression, and click on the **Validate Expression** to ensure the expression is as per the supported format and understand it in human readable form through description.

Timer Maintenance – Timer Details (Edit)



Field Description

Field Name	Description
Timer ID	Name of event for which timer is to be set.
Enabled	Enable or disable the switch to activate or deactivate the timer.
Expression	Specify the expression for the selected event. The format to set the timer is <**Seconds> <Minutes> <Hours> <Day of Month Month> <Day Of Week> <Year>**. Note: 1) Click the ⓘ icon to view the expression format. 2) Click the Validate Expression to execute the expression and validate it.
Description	Displays the expression details.

6. Edit the required details.
7. Click **Save** to update the changes.
   OR
   Click **Back** to navigate back to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.
8. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Back** to go to previous screen.
   OR
   Click **Cancel** to cancel the transaction.
9. The success message of modification appears.
   Click **OK** to complete the transaction.

FAQ

1. **List the supported valid range and allowed special characters in Cron expression parts?**

   Below is the list of supported valid range and allowed special characters in Cron expression parts,

Part	Valid Range	Allowed Special Chars
Second	0-59	*, /
Minute	0-59	*, /
Hour	0-23	*, /
Day Of Month	1-31	*,/, ?
Month	1-12 or JAN-DEC	*,/
Day Of Week	1-7 or SUN – SAT	*,/,?
Year	1970 - 2099	*,/

   Format is,

   <Second><SPACE><Minute><SPACE><Hour><SPACE><DayOfMonth><SPACE><Month><SPACE><DayOfWeek><SPACE><Year>

   Ex:

Cron Expression	Description
* */5 * * JAN ? *	Every Second, Every 5 minute starting from 0 minute, every hour, every day on Jan month, every year
* 10/5 * * JAN ? *	Every Second, Every 5 minute starting from 10 minute, every hour, every day on Jan month, every year
0 0 5/2 * * ? *	At 0 second, at 0 minute, every 2 hour starting from 5 hour, every day every month every year
0 0 5/2 ? * ? *	Invalid Cron Expression, specifying both day of month and day of week not supported
0 0 5/2 * * * *	Invalid Cron Expression, specifying both day of month and day of week not supported

Note:
1) Support for specifying both a day-of-week AND a day-of-month parameter is not implemented within the Quartz framework which is core of OBDX Timer Framework.
2) Special character like L, W, #, Comma, Hyphen are currently not supported by OBDX Timer Framework.

25. First Time Login

Whenever a new user logs into the application for the first time with the user name and password provided by bank, there are certain tasks that he/she needs to fulfil before being able to access the online services of the bank. These steps are configured by Bank and can include accepting Terms and Conditions, Setting up Security Question, My profile and limit information.

The first time login event are configurable at Entity Level. Bank Admin would be able to define the mandatory and skippable steps for each entity.

Post first time login to the application , system will check the configured steps for the logged in entity and will be displayed to user. Once the user completes the first time login steps for his primary entity, and switches to another entity, system will check if the user has completed the first time login steps for the switched entity, if not system will ask the user to complete the same for the switched entity.

Note:

Each step will either have Next or Skip button basis on the configuration (mandatory/optional) done by Bank Administrator.

User will be allowed to skip Non-Mandatory Steps.

Pre-Requisites

- Transaction access is provided to System Administrator.
- Enterprise roles are maintained in application.
- Touch point groups are maintained, if required.
- Limit packages are maintained.

Features Supported In Application

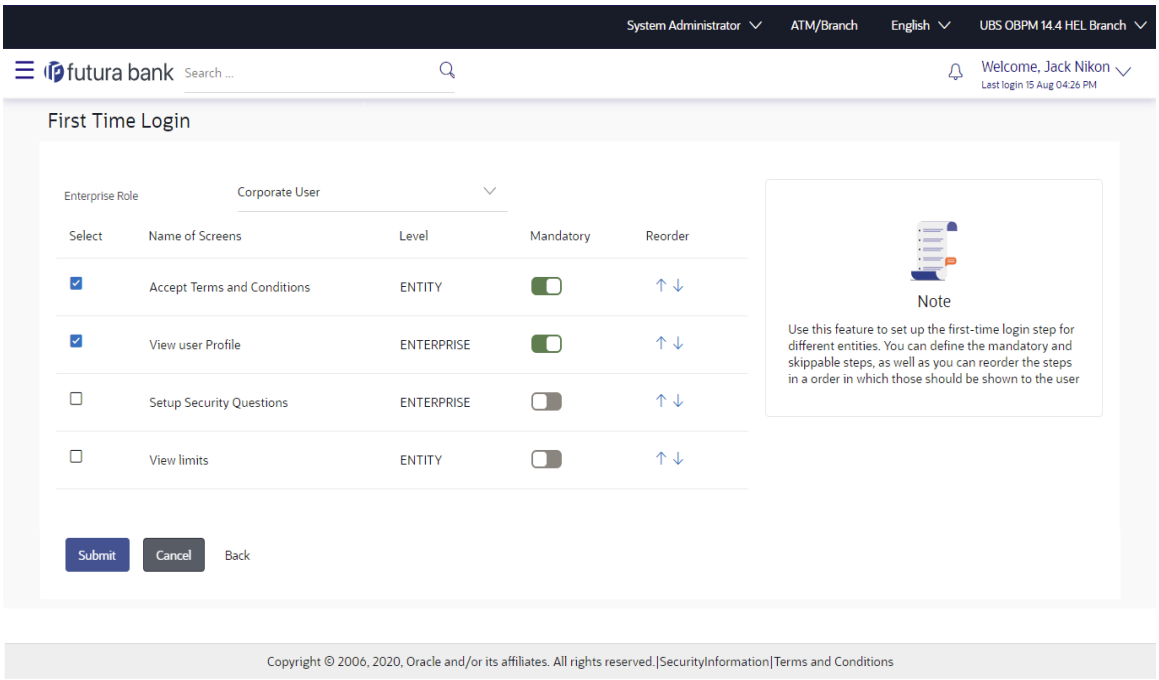
This option allows the System Administrator to:

- Maintain First Time Login Event
- View First Time Login Event
- Edit First Time Login Event

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Configuration > First Time Login

First Time Login



Field Description

Field Name	Description
Enterprise Role	Name of enterprise roles set in application. The options can be: • Corporate User • Administrator • Retail User On selecting an application role, system rules maintained if any, are shown in editable form.
First Time Login Steps	First time login steps to be followed or not. Administrator can also configure the steps along with the order of the steps that need to be displayed to use
Below field are displayed if the First Time Login Steps option is enabled	
Select	Option to decide whether that transaction is to be displayed as part of the first time login steps.

Field Name	Description
Name of Screen	Name of the transaction which is to be included as part of First Time Login Steps process.
Level	Display the Level for First Time Login event .whether its Entity or Enterprise Level (non-editable)
Mandatory	Option which will decide whether the transaction is mandatory to execute as part of First Time Login Steps process.
Reorder	Order in which the transactions will get displayed when the user logs in for the first time. Administrator can click on the reorder icon and configure the order of steps in which these steps need to be displayed to user.

To set up the First Time Login Steps:

1. In the **First Time Login Steps** field, select the appropriate option.
   a. To include in the **First Time Login Steps** process, select the checkbox(s) against the transaction and configure the steps.
   b. Slide Mandatory option to enabled /disabled the execution of transaction in the **First Time Login Steps** process.
   c. Slide ↑↓ icon to set order in which transaction are executed in the **First Time Login Steps** process.
2. Click **Submit** to save First Time Login events.
   OR
   Click **Cancel** to cancel the transaction.
   The success message appears.
3. The **First Time Login - Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Back** to make the changes if any.
   OR
   Click **Cancel** to cancel the transaction and navigate back to 'Dashboard'.
4. The success message of First Time Login maintenance appears along with the transaction reference number. Click **OK** to complete the transaction.

FAQ

1. **Who can create-edit this maintenance?**

   System Administrator can create and edit this maintenance.

2. **How can I find out first time login checks are granted to a particular role and can I change it?**

   You can select a role and view the first time login checks mapped to the role, you can also edit the type of checks ,reorder it and define it those checks are mandatory or not post login to the application

3. **If user closes the window without completing any mandatory step post first time login in to application , what will be the system behaviour?**

   In case the user closes the window without completing any mandatory step, user will be asked to set up the same in his subsequent login.

ORACLE

26. Transaction Aspects

Using this option, System Administrator can define the aspects for a transaction. Depending on the aspects defined for a transaction through this maintenance, the transaction will be available/ unavailable for selection in the respective maintenance screen.

User can view the aspects for a selected transaction and also edit the aspects i.e. enable/disable the aspects for the selected transaction.

The following aspects are available for a transaction:

- Limits Check
- Approvals
- Grace Period
- Working Window
- Blackout
- 2 Factor Authentication
- Audit
- e-Receipts
- Customer Relationship Matrix

Pre-Requisites

System Administrator has access to the specified transaction

Note: There are certain transactions in the system for which all the aspects are not applicable. In such cases on selection of the transaction, the aspect(s) that are not applicable will not get displayed to user.

Features supported in Application:

- View Transaction Aspects
- Edit Transaction Aspects

How to reach here:

System Administrator Dashboard > Configuration > Transaction Aspects
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Configuration > Transaction Aspects

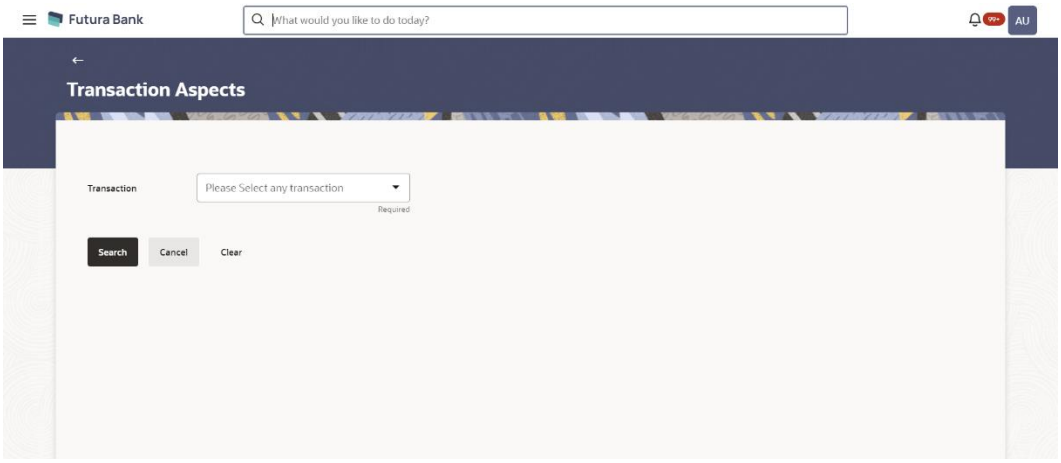
26.1 View Transaction Aspects

System Administrator can view the aspects enabled/disabled for a transaction.

To view the transaction aspects:

1. From the **Transaction** list, select the transaction for which you wish to view the defined aspects.

Transaction Aspects

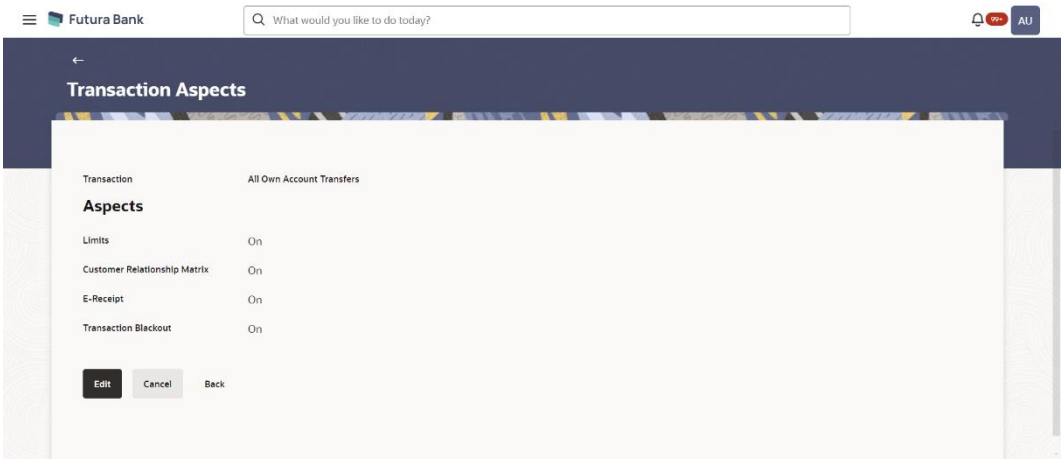


Field Description

Field Name	Description
Transaction	The name of the transaction for which aspects are to be listed.

2. Click **Search**. The **Transaction Aspects- View** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the selected transaction.

Transaction Aspects- View



Field Description

Field Name	Description
Transaction	The name of the transaction for which aspects are to be listed.
Aspects	
List of Aspects	The list of aspects for a transaction.

3. Click **Edit** to modify the aspects.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.

26.2 Update Transaction Aspects

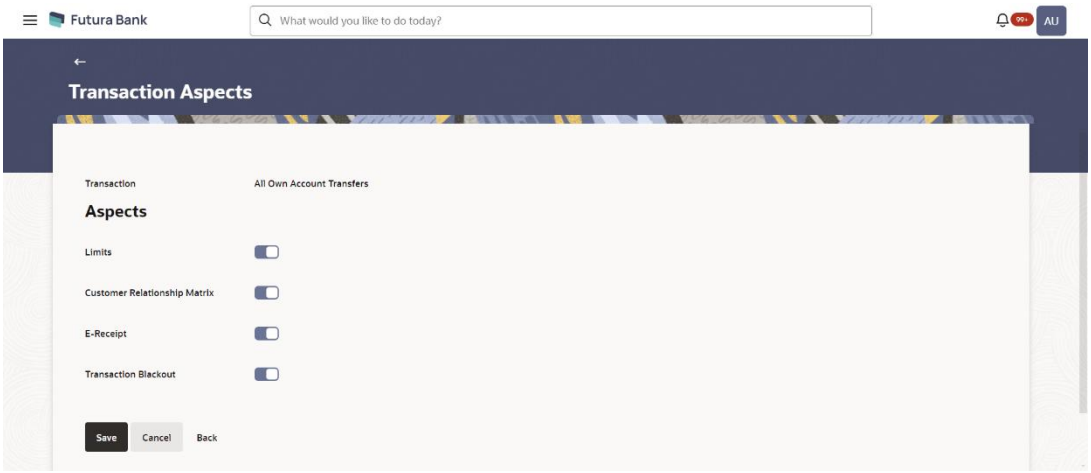
Using this option user can update the listed aspects for a transaction by enabling or disabling it.

To modify the transaction aspects:

1. From the **Transaction** list, select the appropriate transaction.
2. Click **Search**. The Transaction Aspects- View screen appears.
3. Click **Edit** to modify the aspects i.e. the aspect for a transaction can be enabled/disabled. The **Transaction Aspects- Edit** screen appears.

   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.

Transaction Aspects- Edit



Field Description

Field Name	Description
Transaction	The name of the transaction for which aspects are to be updated.
Aspects	
List of Aspects	The list of aspects applicable for the selected transaction.

4. Click on the toggle button against the respective aspect to enable/disable the aspect
5. Click **Save** to confirm the changes.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to make the changes if any. User is directed to the **Transaction Aspects- Edit screen** with values in editable form.
   OR
   Click **Cancel** to cancel the transaction.
7. The success message appears confirming the modification of aspects for the transaction.

27. ATM / Branch Maintenance

ATM Branch Locator feature available to the bank customers enables the users to locate the bank's ATMs/ branches available within a specific radius of his current location.

Default radius is 2.5 Kms which can be configured by updating the value of DEFAULT_SEARCH_RADIUS in digx_fw_config_all_b. Changed value will be in effect post server restart.

For the customers, to fetch the relevant information related to ATMs and Branches, System Administrator maintains the data at their local databases. The details of ATMs and Branches are fetched from the core banking application, which is further enriched and stored in local database. This is a one-time activity at the time of implementation. Subsequently, as and when branches and ATMs are added, or any details regarding them updated, the administrator performs the necessary updates to the bank database.

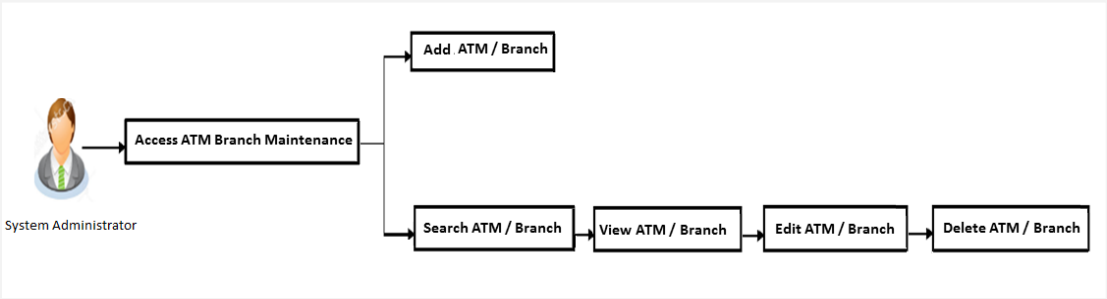
Using this option, the System Administrator can search and view the ATM/ branch and its details (Fetched from core banking application) which include branch/ ATM ID, branch name, address details, phone number, work timings and services offered by the bank. New ATM and branch details can also be manually added, viewed and edited.

The System Administrator can manually add new branch/ ATM details one by one, or add multiple branches / ATMs details simultaneously through file upload.

Pre-requisites

- Transaction access is provided to System Administrator.
- Approval rule set up for System Administrator to perform the actions.
- ATM and Branches are maintained in core banking application.

Workflow



Features Supported In Application

- Add ATM/ branches
- View ATM/ branches
- Edit ATM/ branches
- Delete ATM / branches

How to reach here:

System Administrator Dashboard > Configuration > ATM/ Branch Maintenance
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Configuration > ATM/ Branch Maintenance

27.1 ATM/ Branch Maintenance - Search

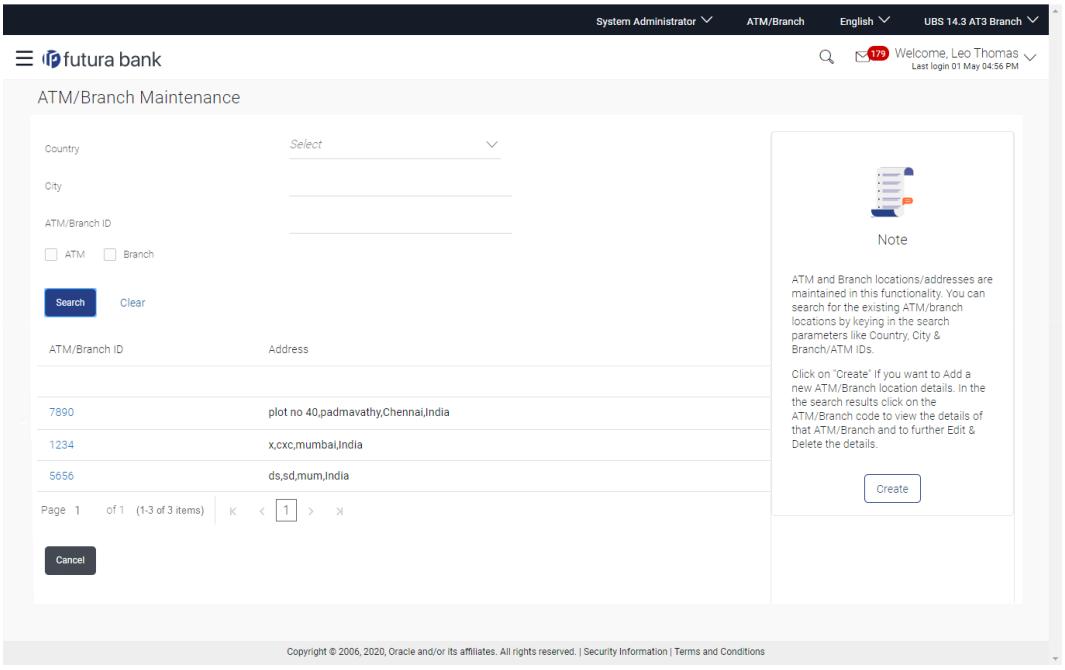
Using this option, System Administrator can search for particular ATM/ Branch based on search parameters. The search results display a list of ATM/ Branch corresponding to the search inputs.

If the search parameters are not specified, records of all the limits maintained in the application are displayed.

To search the ATM/ branch:

1. Click **Search**. The **ATM/ Branch Maintenance** screen with search results appears based on the searched criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.

ATM/ Branch Maintenance - Search

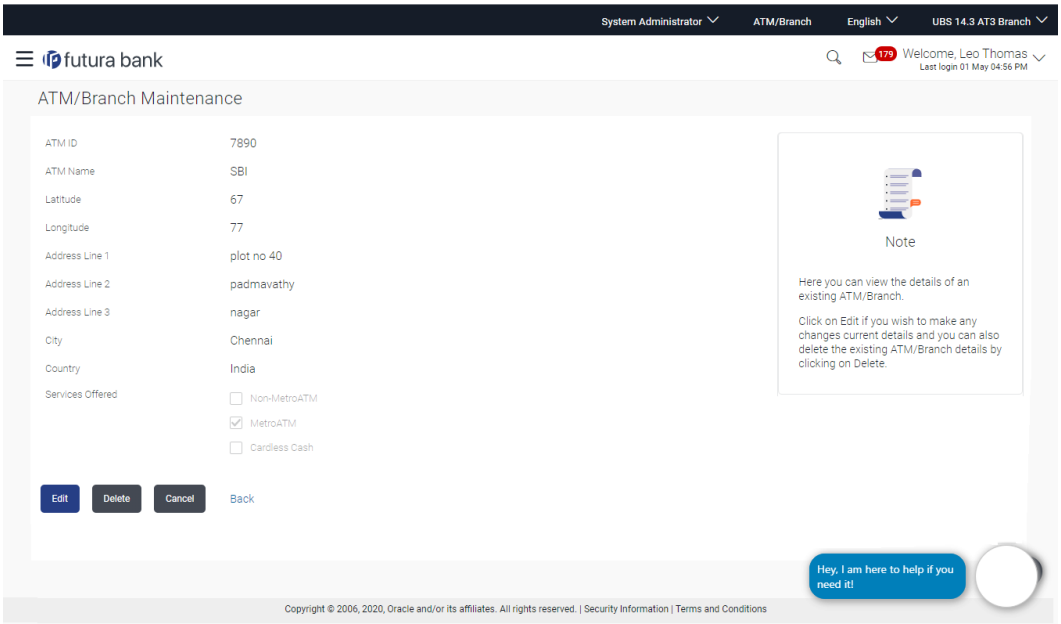


Field Description

Field Name	Description
Country	Select the country in which you want to locate a branch or ATM of the bank.
City	Select the city in which you want to locate a branch or ATM of the bank.
ATM/ Branch ID	Unique key to identify the ATM / Branch. Specify valid Branch / ATM ID maintained in the system.
ATM/ Branch	Select if the search is for a branch or ATM.
Search Result	
ATM/ Branch ID	Unique key of the ATM / Branch.
Address	The address of the ATM / branch that corresponds with the ATM / branch ID.

2. View the search results. Click the **ATM/ Branch ID** link of the record for which you want to view the details. The **ATM/ Branch Maintenance - View** screen appears.

ATM/ Branch Maintenance - View



Field Description

Field Name	Description
ATM/ Branch ID	Unique key to identify the ATM / branch.
ATM/ Branch Name	Name of the ATM / branch.
Latitude	The location of the ATM/ branch in term of latitude which is the angular distance, north or south of the equator (an imaginary circle around the Earth halfway between the North Pole and the South Pole).
Longitude	The location of the ATM/ branch in term of longitude which is angular distance, east or west of the prime meridian (an imaginary line running from north to south through Greenwich, England).
Address Line 1 - 4	The address of the ATM / branch that corresponds with the ATM / branch ID.
City	The city of the ATM / branch that corresponds with the ATM / branch ID.
Country	The country of the ATM / branch.
Work Timings	The operating hours of the branch / ATM. This field appears if you are viewing the details of a **Branch of the bank.**
Additional Details	Additional details if any. This field appears if you are viewing the details of a **Branch of the bank.**
Phone Number	The phone number of the branch / ATM. This field appears if you are viewing the details of a **Branch of the bank.**
Services Offered	The services offered by the bank branch / ATM.

3. Click **Edit** to edit the ATM/ branch details.
   OR
   Click **Delete** to delete the ATM/ branch details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.

27.2 ATM/ Branch Maintenance - Add

Using this option, System Administrator can add ATM or branch details. Single ATM/ branch details can be added directly using the Add ATM/ branch Details screen. Multiple ATMs or branches can be added by uploading a File.

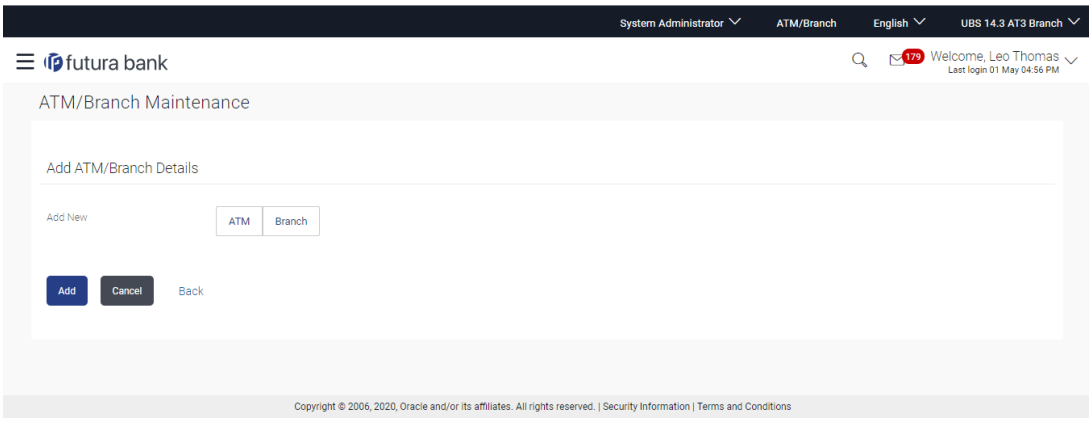
Adding ATM/ branches feature allows the bank administrator to:

- Add Single ATM/ Branches
- Add Multiple ATM/ Branches

To add an ATM/ Branch:

1. Navigate to the **ATM/Branch Maintenance** screen.
2. Click **Create**.
   The **ATM/ Branch Maintenance - Add ATM/ Branch Details** screen appears.

ATM/ Branch Maintenance - Add Single ATM/ Branch Details

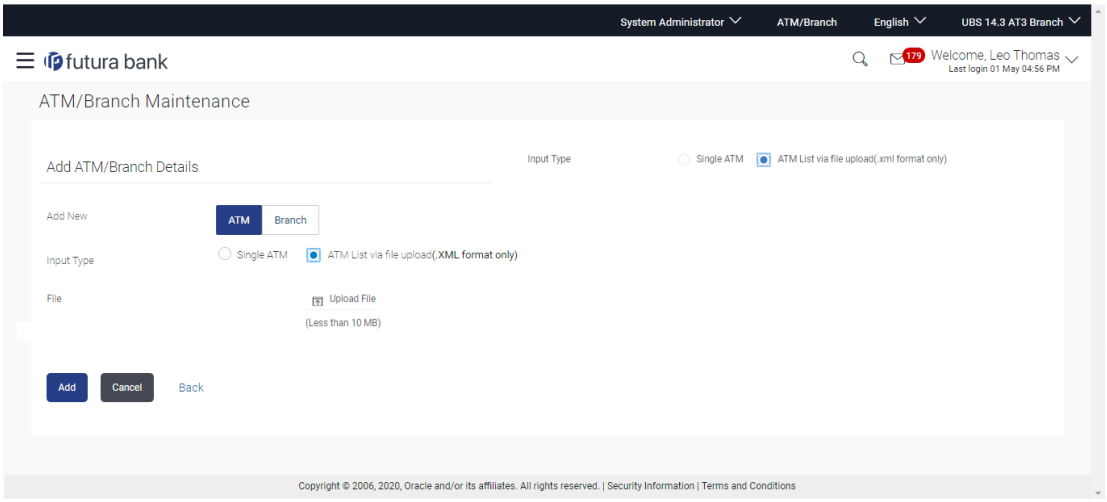


Field Description

Field Name	Description
Add ATM/ Branch Details	
Add New – ATM / Branch	Buttons to be selected for adding either the ATM or the branch details. The buttons are: • ATM • Branch

3. In the **Add New** field, click the appropriate button to add the ATM or branch details.
   The **ATM/ Branch Maintenance - Add ATM/ Branch Details** screen with options to add single or multiple ATM/ Branch details appear.

ATM/ Branch Maintenance - Add ATM/ Branch Details

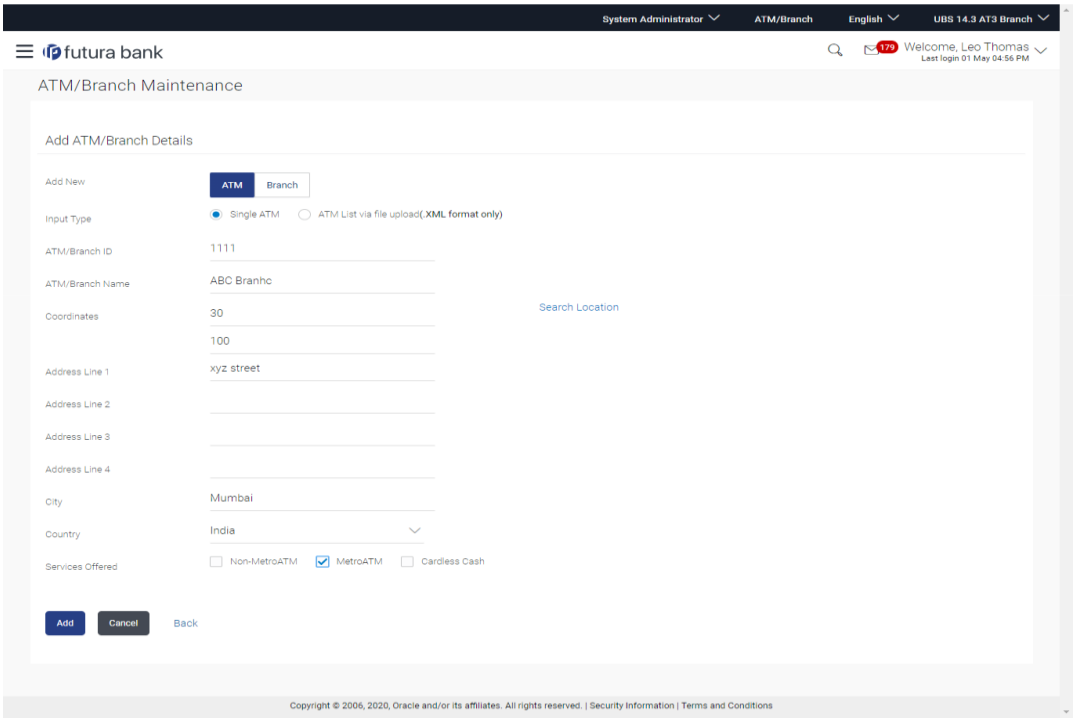


Field Description

Field Name	Description
Add New – ATM / Branch	Buttons for adding either the ATM or the branch details.
Input Type	Options to add single or multiple ATM/ branch details. • Add Single ATM/ Branches • Add Multiple ATM/ Branches
File	Select the file to be uploaded.

4. In the **Input Type** field, click the appropriate option to add the single or multiple ATM/ branch details.
   a. If you select **Single ATM/ Branches** option, the fields for adding the details appears on the **ATM/ Branch Maintenance - Add ATM/ Branch Details** screen.

Add Single ATM/ Branches Details



Field Description

Field Name	Description
Add ATM/ Branch Details	
Add New – ATM / Branch	Buttons for adding either the ATM or the branch details.
Input Type	Options to add single or multiple ATM/ branch details. • Single ATM/ Branch • Multiple ATMs/ Branches via file upload (.xml format only)
ATM/ Branch ID	Unique key to identify the ATM / branch.
ATM/ Branch Name	Name of the ATM / branch which is to be added.
Coordinates	The location of the new ATM/ branch in term of latitude which is the angular distance, north or south of the equator (an imaginary circle around the Earth halfway between the North Pole and the South Pole).

Field Name	Description
	The location of the new ATM/ branch in term of longitude which is angular distance, east or west of the prime meridian (an imaginary line running from north to south through Greenwich, England). Click the **Search Location** link to auto populate the coordinates value.
Address Line 1 - 4	The address of the ATM / branch that corresponds with the ATM / branch ID.
City	The city in which a branch or ATM of the bank is located.
Country	The country a branch or ATM of the bank is located.
Work Timings	The operating hours of the branch This field appears if you click **Branch** button in the **Add New** field.
Additional Details	Additional details if any. This field appears if you click **Branch** button in the **Add New** field.
Phone Number	The phone number of the branch / ATM. This field appears if you click **Branch** button in the **Add New** field.
Alternate Phone Number	A contact number other than your main phone number, if you have any. This field appears if you click **Branch** button in the **Add New** field.
Services Offered	Services offered by the bank. Following services are offered if you click **ATM** button in the **Add New** field. (The information will be fetched based on the data maintained as Day 0). • Non-Metro ATM • Metro ATM • Cardless Cash Following services are offered if you click **Branch** button in the **Add New** field. (The information will be fetched based on the data maintained as Day 0). • Wealth branch • Loan Servicing Branch • Forex Branch • Gold Loan Branch • Touch Banking Branch • Lockers Enabled Branch

Field Name	Description
	• Retail Branch

b. In the **ATM/ Branch ID** field, enter the unique id for ATM/ branch.

c. In the **ATM/ Branch Name** field, enter the name of the new ATM/ branch.

d. In the **Coordinates** field, click the **Search Location** link to enter the location. The coordinate value appears in the field.

e. In the **Address Line 1, 2** field, enter the address of the new ATM/ branch.

f. In the **City** field, enter the city of the ATM/ branch.

g. From the **Country** list, select the country of the new ATM/ branch.

h. In the **Phone Number** field, enter the phone number of the bank branch.

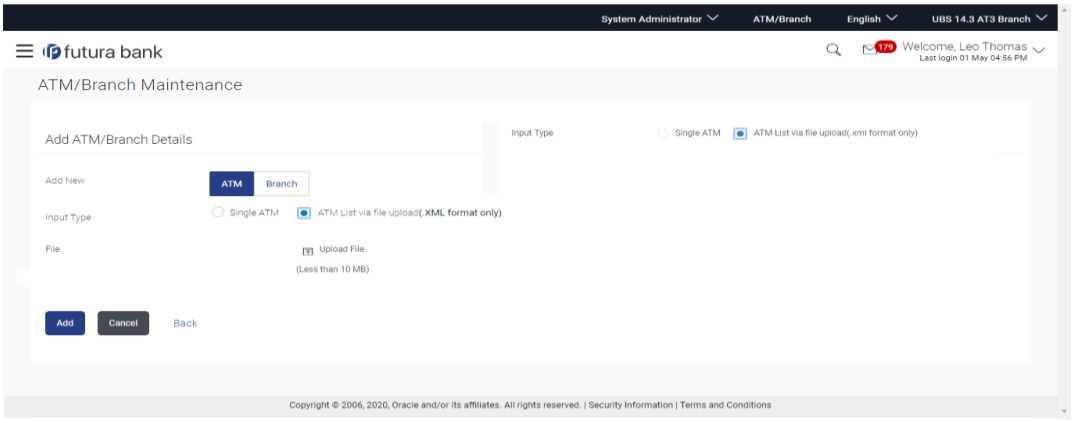
i. Click **Add** to add the ATM/ branch details.
OR
Click **Cancel** to cancel current transaction.

j. The **Add ATM/ Branch Details - Review** screen appears post necessary validations. Verify the details, and click **Confirm**.
OR
Click **Edit** to make the changes if any.
User is directed to the **Add ATM/ Branch Details** screen with values in editable form.
OR
Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.

k. The success message of saving the ATM/ Branch maintenance appears along with the transaction reference number and status of the transaction.
Click **OK** to complete the transaction and navigate back to 'Dashboard'.

5. In the **ATM/ Branch Maintenance - Add Branch Details** screen, if you select **Multiple ATM/ Branches** option, the **ATM/ Branch Maintenance - Add ATM/ Branch Details** screen for uploading the files appears.

ATM/ Branch Maintenance - Add Multiple ATM/ Branch Details



Field Description

Field Name	Description
Add ATM/ Branch Details	
Add New	Buttons to be selected for adding either the ATM or the branch details.
Input Type	Options to add single or multiple ATM/ branch details. • Single ATM/ Branch • Multiple ATM/ Branches
File	Select the file to be uploaded.

6. In the **Input Type** field, click the appropriate option to add the single or multiple ATM/ branch option.
   a. If you select **Multiple ATM/ Branches** option, the fields for uploading file (specific file format is mentioned here – XML only) appears on the **ATM/ Branch Maintenance - Add ATM/ Branch Details** screen.
   b. In the **File** field, select the file to be uploaded.
   c. Click **Add** to add the ATM/ branch details.
      OR
      Click **Cancel** to cancel current transaction.
   d. The **Add ATM/ Branch Details - Review** screen appears post necessary validations. Verify the details, and click **Confirm**.
      OR
      Click **Edit** to make the changes if any.
      User is directed to the **Add ATM/ Branch Details** screen with values in editable form.
      OR
      Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   e. The success message of saving the ATM/ Branch maintenance appears along with the transaction reference number and status of the transaction.
      Click **OK** to complete the transaction and navigate back to 'Dashboard'.

ATM file template example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ATMs xmlns:datatype="http://datatype.fc.ofss.com" xmlns:validationdtoapp="http://validation.dto.app.fc.ofss.com" xmlns:dtocommondomainframework="
http://dto.common.domain.framework.fc.ofss.com" xmlns:ns4="http://enumeration.fc.ofss.com">
    <ATM>
        <coordinates>
            <latitude>19.1547995</latitude>
            <longitude>72.8562558</longitude>
        </coordinates>
        <ID>DBA001</ID>
        <name>Demo Bank Branch1</name>
        <PostalAddress>
            <datatype:city>Mumbai</datatype:city>
            <datatype:country>INDIA</datatype:country>
            <datatype:line1>Line1</datatype:line1>
            <datatype:line2>Line2</datatype:line2>
        </PostalAddress>
        <Services>
            <id>3</id>
        </Services>
        <Services>
            <id>2</id>
        </Services>
        <type>ATM</type>
    </ATM>
    <ATM>
        <coordinates>
            <latitude>19.16</latitude>
            <longitude>72.86</longitude>
        </coordinates>
        <ID>DBA002</ID>
        <name>Demo Bank Branch2</name>
        <PostalAddress>
            <datatype:city>Nagpur</datatype:city>
            <datatype:country>INDIA</datatype:country>
            <datatype:line1>Line1</datatype:line1>
            <datatype:line2>Line2</datatype:line2>
        </PostalAddress>
        <Services>
            <id>5</id>
        </Services>
        <Services>
            <id>2</id>
        </Services>
        <type>ATM</type>
    </ATM>
</ATMs>
```

Output

```
1547995 72.8562558 DBA001 Demo Bank Branch1 Mumbai INDIA Line1 Line2 3 2 ATM 19.16 72.86 DBA002 Demo Bank Branch2 Nagpur INDIA Line1 Line2 5 2 ATM
```

Branch file template example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Branches xmlns:datatype="http://datatype.fc.ofss.com" xmlns:validationdtoapp="http://validation.dto.app.fc.ofss.com" xmlns:dtocommondomainframework="
http://dto.common.domain.framework.fc.ofss.com" xmlns:ns4="http://enumeration.fc.ofss.com">
  <!-- Sample Record to Upload branch -->
<Branch>
        <coordinates>
            <latitude>17.900840</latitude>
            <longitude>102.5332620</longitude>
        </coordinates>
        <ID>STBRECORD01</ID>
        <name>ST Bank KM8</name>
        <PostalAddress>
            <datatype:city>Vientiane</datatype:city>
            <datatype:country>LAO PEOPLES DEMOCRATIC REPUBLIC</datatype:country>
            <datatype:line1>Somvang Village</datatype:line1>
            <datatype:line2>Hadsayfong District</datatype:line2>
        </PostalAddress>
        <Services>
            <id>1</id>
        </Services>
        <Services>
            <id>7</id>
        </Services>
        <type>BRANCH</type>
        <phone>
            <number>021-315712</number>
        </phone>
        <workDays>Mon-Fri</workDays>
        <Timings>09:00-17:00</Timings>
        <!-- In case of multiple branch timings required -->
        <workDays>Sat</workDays>
        <Timings>09:00-17:00</Timings>
    </Branch>

    <Branch>
        <coordinates>
            <latitude>17.900840</latitude>
            <longitude>102.5332620</longitude>
        </coordinates>
        <ID>STBRECORD02</ID>
        <name>ST Bank KM8</name>
        <PostalAddress>
            <datatype:city>Vientiane</datatype:city>
            <datatype:country>LAO PEOPLES DEMOCRATIC REPUBLIC</datatype:country>
            <datatype:line1>Somvang Village</datatype:line1>
            <datatype:line2>Hadsayfong District</datatype:line2>
        </PostalAddress>
        <Services>
            <id>1</id>
        </Services>
        <Services>
            <id>7</id>
        </Services>
        <type>BRANCH</type>
        <phone>
            <number>021-315712</number>
        </phone>
        <workDays>Mon-Fri</workDays>
        <Timings>09:00-17:00</Timings>
        <!-- In case of multiple branch timings required -->
        <workDays>Sat</workDays>
        <Timings>09:00-17:00</Timings>
    </Branch>

</Branches>
```

Output

17.900840 102.5332620 STBRECORD01 ST Bank KM8 Vientiane LAO PEOPLES DEMOCRATIC REPUBLIC Somvang Village Hadsayfong District 1 7 BRANCH 021-315712 Mon-Fri 09:00-17:00 Sat 09:00-17:00 17.900840 102.5332620 STBRECORD02 ST Bank KM8 Vientiane LAO PEOPLES DEMOCRATIC REPUBLIC Somvang Village Hadsayfong District 1 7 BRANCH 021-315712 Mon-Fri 09:00-17:00 Sat 09:00-17:00

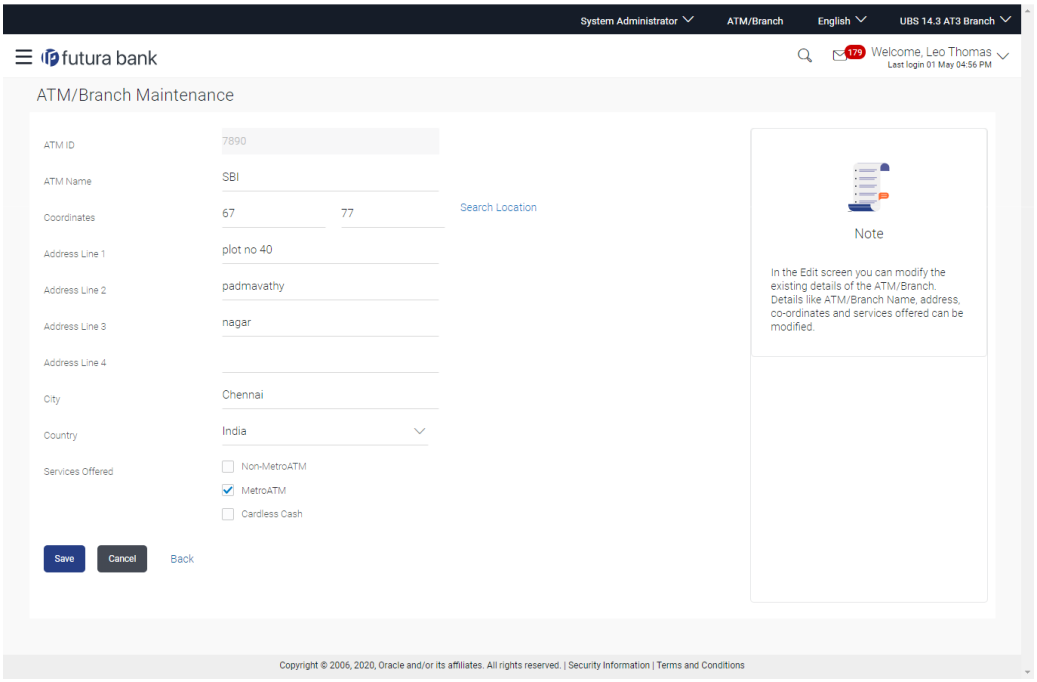
27.3 ATM/ Branch Maintenance - Edit

Using this option, System Administrator can update or edit an ATM/ branch details.

To edit an ATM/ branch details:

1. In the **ATM/ Branch Maintenance** screen, click **Search**. The **ATM/ Branch Maintenance** screen with search results appears based on the search criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.
2. Click the **ATM/ Branch ID** link of the record for which you want to view the details. The **ATM/ Branch Maintenance - View** screen appears.
3. Click **Edit** to edit the ATM/ branch details. The **ATM/ Branch Maintenance - Edit** screen appears.

ATM/ Branch Maintenance - Edit



Field Description

Field Name	Description
ATM/ Branch ID	Unique key to identify the ATM / branch. This field is not editable.

Field Name	Description
ATM/ Branch Name	Name of the ATM / branch which is to be edited.
Latitude	The location of the ATM/ branch in term of latitude which is the angular distance, north or south of the equator (an imaginary circle around the Earth halfway between the North Pole and the South Pole).
Longitude	The location of the ATM/ branch in term of longitude which is angular distance, east or west of the prime meridian (an imaginary line running from north to south through Greenwich, England).
Address Line 1 - 4	The address of the ATM / branch that corresponds with the ATM / branch ID.
City	The city of the ATM / branch that corresponds with the ATM / branch ID.
Country	The country of the ATM / branch.
Work Timings	The operating hours of the branch / ATM. This field is only applicable when the user is editing details of the **Branch**.
Additional Details	Additional details if any. This field appears if you are viewing the details of a **Branch of the bank.**
Phone Number	The phone number of the branch / ATM. This field is only applicable when the user is editing details of the **Branch**.
Services Offered	The services offered by the bank branch/ ATM.

4. In the **ATM/ Branch Name** field, edit the name of the new ATM/ branch if required.
5. In the **Coordinates** field, click the **Search Location** link to enter the location. The coordinate value appears in the field. Modify, if required.
6. In the **Address Line 1, 2** field, edit the address of the new ATM/ branch if required.
7. In the **City** field, edit the city of the ATM/ branch (if required).
8. From the **Country** list, select the country of the new ATM/ branch.
9. In the **Phone Number** field, edit the phone number of the bank branch if required.
10. Click **Save** to update the ATM/ branch details.
    OR
    Click **Cancel** to cancel current transaction.
    OR
    Click **Back** to navigate back to previous screen.

11. The **Edit ATM/ Branch Details - Review** screen appears post necessary validations. Verify the details, and click **Confirm**.
    OR
    Click **Edit** to make changes if any.
    User is directed to the **Edit ATM/ Branch Details** screen with values in editable form.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
12. The success message of saving the ATM/ Branch maintenance appears along with the status of the transaction.
    Click **OK** to complete the transaction and navigate back to 'Dashboard'.

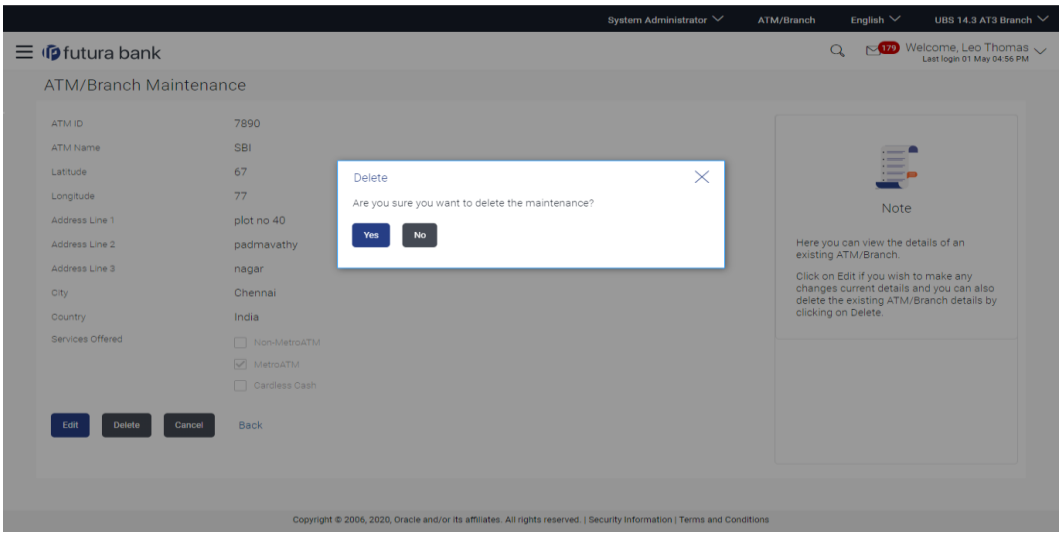
27.4 ATM/ Branch Maintenance - Delete

The System Administrator can delete the ATM and branch details.

To delete ATM/ branch details:

1. In the **ATM/ Branch Maintenance** screen, click **Search**. The **ATM/ Branch Maintenance** screen with search results appears based on the search criteria.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process.
2. Click the **ATM/ Branch ID** link of the record for which you want to view the details. The **ATM/ Branch Maintenance - View** screen appears.
3. Click **Delete** to delete the ATM/ branch details.
   The application will prompt the administrator with a deletion message with an option of Yes / No.

ATM/ Branch Maintenance - Delete



4. Click **Yes** to delete ATM / Branch. It will navigate to confirmation page with a success message and the status.
   OR
   Click **No** if you do not wish to delete the ATM / Branch.
5. Click **OK** to complete the transaction.

FAQ

1. In which format I can upload a file with ATM and Branch details?

You can upload a file in xml format to add new branches and ATMs.

2. Do I need to remember the latitude and longitude while updating single ATM/Branch?

No, you may search the location. Based on the location selected latitude and longitude data will be auto fetched and shown on the screen.

3. Can I edit the address and other details of already saved ATM/Branch?

Yes, an option to edit the information of already saved ATM/Branches is provided.

28. Product Mapping

Product mapping feature allows the System Administrator to map products to users from the channel.

System Administrator can map products maintained in the core banking system to different User type and all the users falling under that user type can open accounts for the mapped products only. This option is currently enabled for Term Deposit and Recurring Deposit module.

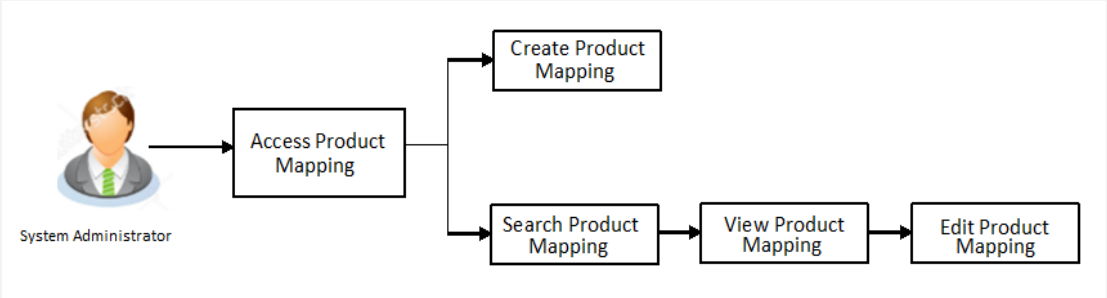
For example: A user can open a term deposit or a recurring deposit only under those products which are mapped to the User Type/User Segment assigned to the user. Products which are not mapped, will not be available (for opening deposit accounts) to a channel user. This will be a part of Day 1 setup.

Note: For User Type – Retail, product mapping can be done for User Type and User Segment combination.

Pre-Requisites

- Transaction access is provided to System Administrator.
- Approval rule is set up for System Administrator to perform the actions.
- Necessary products are maintained in core banking application.

Workflow



Features Supported In Application

The module supports following features:

- View Product Mapping
- Edit Product Mapping
- Create Product Mapping

How to reach here:

System *Administrator Dashboard > Configuration > Product Mapping*
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Configuration > Product Mapping

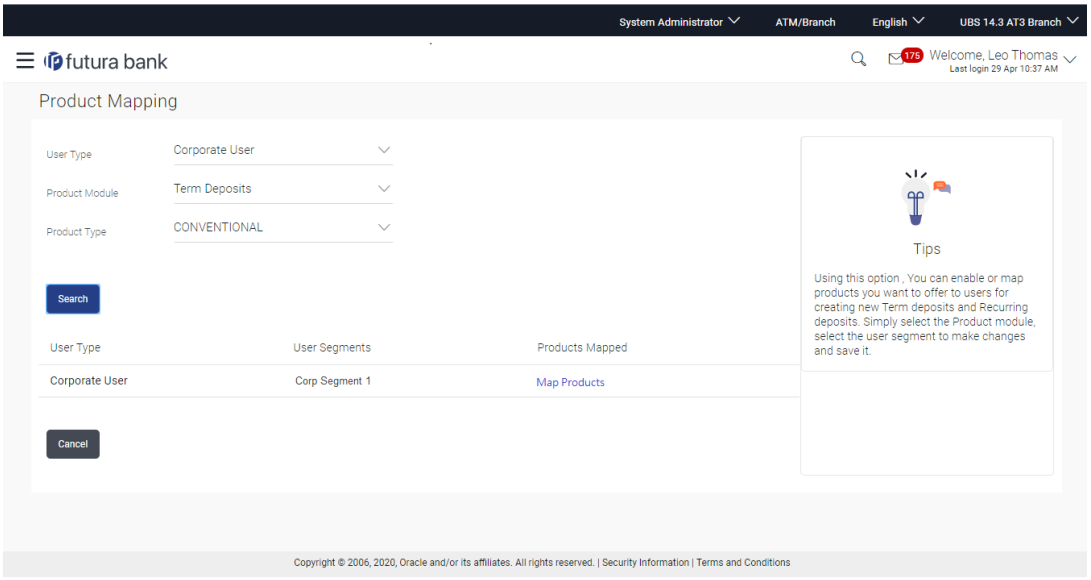
28.1 Product Mapping - View

Using Product mapping view option, System Administrators can view the list of products mapped to the product module. The System Administrator can view the mapping details by clicking the User Segments link.

To view the product mapping:

8. Navigate to the **Product Mapping** screen. The **Product Mapping** screen with mapped products appears.
   OR
   Click **Cancel** to cancel the transaction and navigate to the dashboard.

Product Mapping



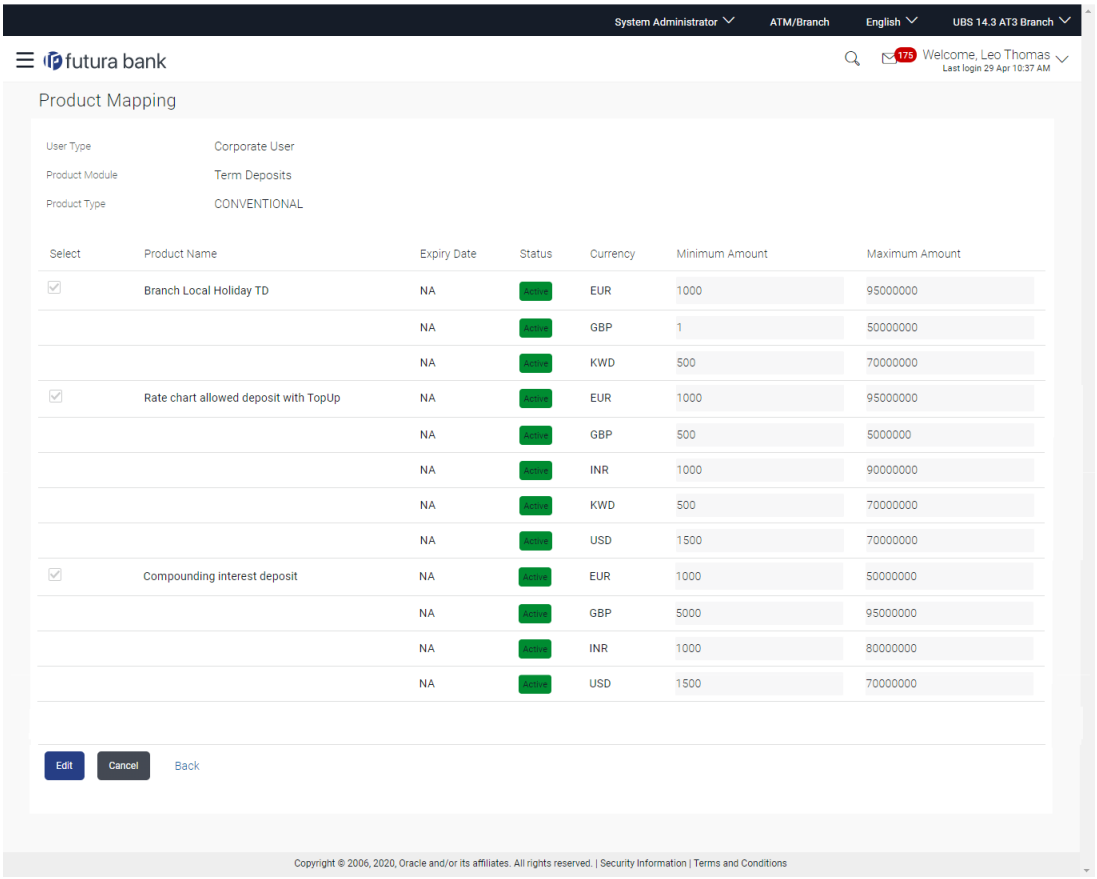
Field Description

Field Name	Description
User Type	The user type available for mapping products.
Product Module	Following product modules are available for mapping: • Term Deposit • Recurring Deposit
Product Type	The type of products available to be mapped to the user segment or to the role for that product module.
Search Result	

Field Name	Description
User Type	The user for which products are mapped.
User Segment	The user segments for which products mapped. This field is applicable only for Retail user type.
Products Mapped	The number of products mapped to the user segment or user type for that product type and product module.

9. Click the **Product Mapped** link of the user record for which you want to view the details. The **Product Mapping - View** screen appears.

Product Mapping - View



Field Description

Field Name	Description
View	
User Type	The user for which products are mapped.
Product Module	Following product modules are available for mapping: • Term Deposit • Recurring Deposit Note: For corporate only Term Deposit product module is available
Product Type	The type of product under the selected module for which the product list needs to be fetched .
User Segment	The user segment for which products are mapped. This field is applicable only for Retail user type.
Product Name	Name of the product which is mapped to the user type for the selected product type and product module.
Expiry Date	The expiry date of the product. If the product is expired, an 'Expired' flag is shown against the product.
Status	The current status of the product.
Currency	The currency in which products are maintained.
Minimum Amount	The minimum permissible amount for opening deposit under the selected product.
Maximum Amount	The maximum permissible amount for opening deposit under the selected product.

10. Click **Edit** to edit the user-segment - product mapping.
    OR
    Click **Cancel** the operation and navigate to the 'Dashboard'.
    OR
    Click **Back** to navigate to the previous screen.

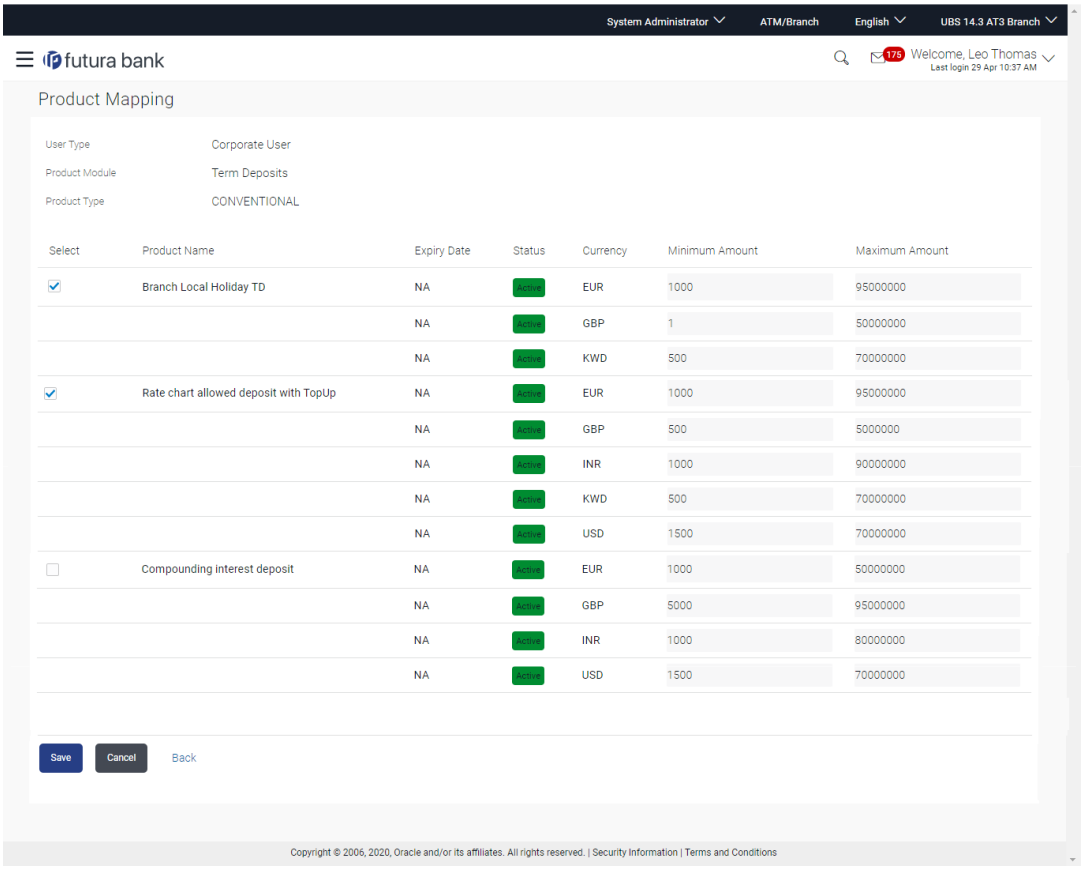
28.2 Product Mapping - Edit

This function enables the System Administrator to edit the product mapping. The System Administrator can map or delete the products to the product module.

To edit or update the product mapping:

11. In the **Product Mapping** screen, click the **Product Mapped** link of the user record for which you want to edit the details.
    The **Product Mapping - View** screen appears.
12. Click **Edit** to edit the user-segment - product mapping. The **Product Mapping – Edit** screen appears.
    OR
    Click **Cancel** the operation and navigate to the 'Dashboard'.
    OR
    Click **Back** to navigate to the previous screen.

Product Mapping - Edit



Field Description

Field Name	Description
Edit	
User Type	The user for which products are mapped.
Product Module	One of the following product modules for which the mapping is to be edited: • Term Deposit • Recurring Deposit
Product Type	The list of product type, available for mapping.
User Segment	The user segment, for which products are mapped.
Product Name	Name of the product which is mapped to the user type for the selected product type and product module.
Expiry Date	The expiry date of the product. If the product is expired, an 'Expired' flag is shown against products.
Status	The current status of the product.
Currency	The currency in which products are maintained.
Minimum Amount	The minimum permissible amount for opening deposit under the selected product.
Maximum Amount	The maximum permissible amount for opening deposit under the selected product.

13. Edit View the defined values for fields, in an editable form.
14. Edit the required details.
15. Click **Save** to save the changes.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
    OR
    Click **Back** to navigate to previous screen.
16. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to previous screen.

17. The success message of transaction submission appears along with the transaction reference number and status.
    Click **OK** to complete the transaction.

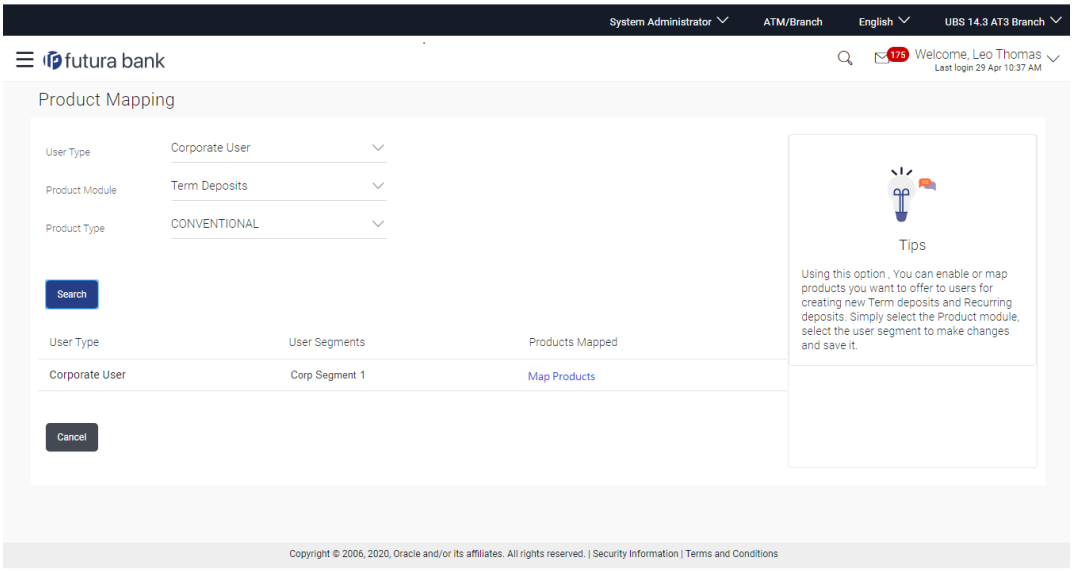
28.3 Product Mapping - Create

This option enables the System Administrator to select the products and map it to the Product Module.

To create a new product mapping:

18. Navigate to the **Product Mapping** screen.
19. Select the User Type for which the product mapping needs to be maintained
20. Select the User Segment (applicable only for Retail user type).

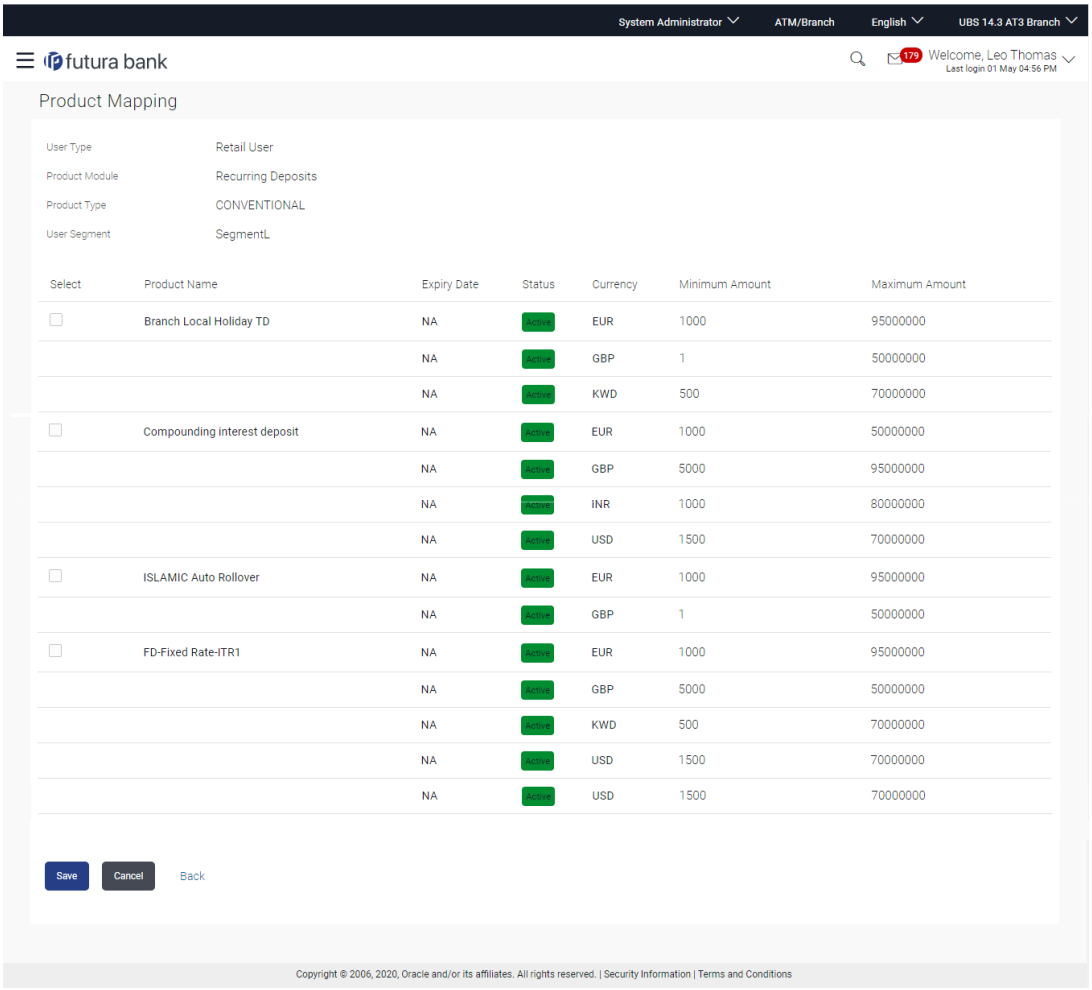
Product Mapping



21. Click **Map Products**.
    The **Product Mapping - Create** screen appears.

Note: The **Map Products** link is available only if no products are mapped to the user segment.

Product Mapping - Create



Field Description

Field Name	Description
Create	
User Type	The user for which products are mapped.
Product Module	Following product modules are available for mapping: • Term Deposit • Recurring Deposit
Product Type	The list of product, available for mapping.

Field Name	Description
User Segment	The user segment, for which products are to be mapped.
Product Name	Name of the product which is mapped to the user type for the selected product type and product module.
Expiry Date	The expiry date of the product. If the product is expired, an 'Expired' flag is shown against products.
Status	The current status of the product. **Note**: Only the active products are displayed
Currency	The currency in which products are maintained.
Minimum Amount	The minimum permissible amount for opening deposit under the selected product.
Maximum Amount	The maximum permissible amount for opening deposit under the selected product.

22. From the **User Type** list, select user for which products are mapped.
23. From the **Product Module** list, select product modules which are available for mapping.
24. From the Product Type list, select product type available for mapping.
25. Select the checkbox(s) for the product which has to be mapped to the user.
26. In the Minimum Amount field, enter the minimum permissible amount for opening deposit under the selected product.
27. In the Maximum Amount field, enter the maximum permissible amount for opening deposit under the selected product.
28. Click Save to save the mapping.
    OR
    Click Cancel to cancel the operation and navigate back to ‘Dashboard’.
    OR
    Click Back to navigate to previous screen.
29. The Review screen appears. Verify the details, and click Confirm.
    OR
    Click Cancel to cancel the transaction.
    OR
    Click Back to navigate to previous screen.
30. The success message of transaction submission appears along with the transaction reference number and status.
    Click OK to complete the transaction.

FAQ

1. **For which type of products, product mapping functionally is available?**

   As of now, product mapping feature is enabled only for Term Deposit and Recurring Deposit type of products for retail users and Term Deposit for corporate users.

2. **Can customer view the account details of an account opened under a product which is not mapped?**

   Yes, user can view the account details of an account opened under a product which is not mapped. The restriction will only be for opening new account from channel.

3. **What will happen once the products mapped gets expired?**

   The expired products will no longer be available for product mapping. Also customers will not be able to open new accounts using expired product.

4. **What will happen if the products are not mapped to any user segment and are only mapped to user type?**

   In this case, all the products mapped to the user type will be available for account opening to the users associated to that user type.

29. User Profile Maintenance

This function enables the System/Bank Administrator user to manage the user profile details that needs to be shown and needs to be made available for modification for Retail users. Details maintained on user profile includes date of birth, PAN card number, Aadhar number, passport number, national ID, driving license, communication address, email ID, and contact number, fax number, etc.

In a multi entity scenario, Administrator can do this setup for each entity by selecting the entity.

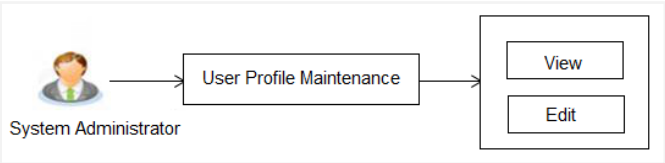
Note: For the business users to be able to modify the 'My Profile' fields, the modification of those fields should be allowed in FCUBS or in the backend Host System.

FCUBS has a separate maintenance for allowing modification of user's details, please make sure that modification of the required user details in enabled (if the FCUBS is configured as a backend system).
This maintenance is only applicable for Retail user.

Pre-requisites

- User must have a valid Login credentials
- Transaction access is provided to system administrator.
- Approval rule set up for Bank administrator to perform the actions.

Workflow



Features supported in application

The administrator can perform the following actions:

- View User Profile
- Edit User Profile

How to reach here:

System/ Bank Administrator Dashboard > Configuration > User Profile Maintenance
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Configuration > User Profile Maintenance

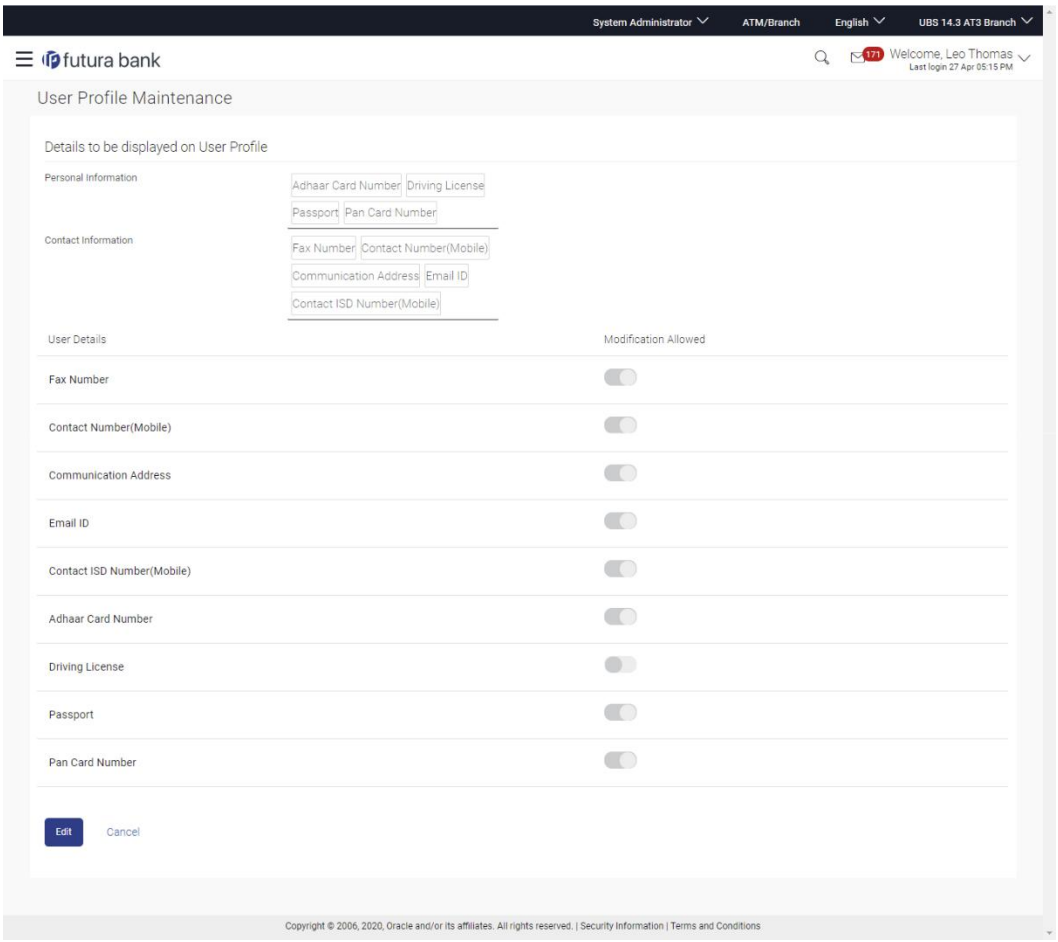
29.1 User Profile - View

This screen displays the setup done for user profile maintenance done for user type –Retail.

To view user profile details:

1. Navigate to the **User Profile Maintenance** screen, the user profile maintained for the user appears.

User Profile Maintenance- View



Field Description

Field Name	Description
User Type	Displays the user type for whom the user profile is to be created. The user can be: • Retail
Details to be displayed on User Profile	
Personal Information	Displays the personal details maintained for the bank/system administrator for being shown to business user on his/her profile. The options against each field are: • Enable: If the toggle is displayed as enabled, that field can be modified by the business user. • Disable: If the toggle is displayed as disabled, that field cannot be modified by the business user.
Contact Information	Displays the contact details maintained for the bank/system administrator for being shown to business user on his/her profile. The options against each field are: • Enable: If the toggle is displayed as enabled, that field can be modified by the business user. • Disable: If the toggle is displayed as disabled, that field cannot be modified by the business user.

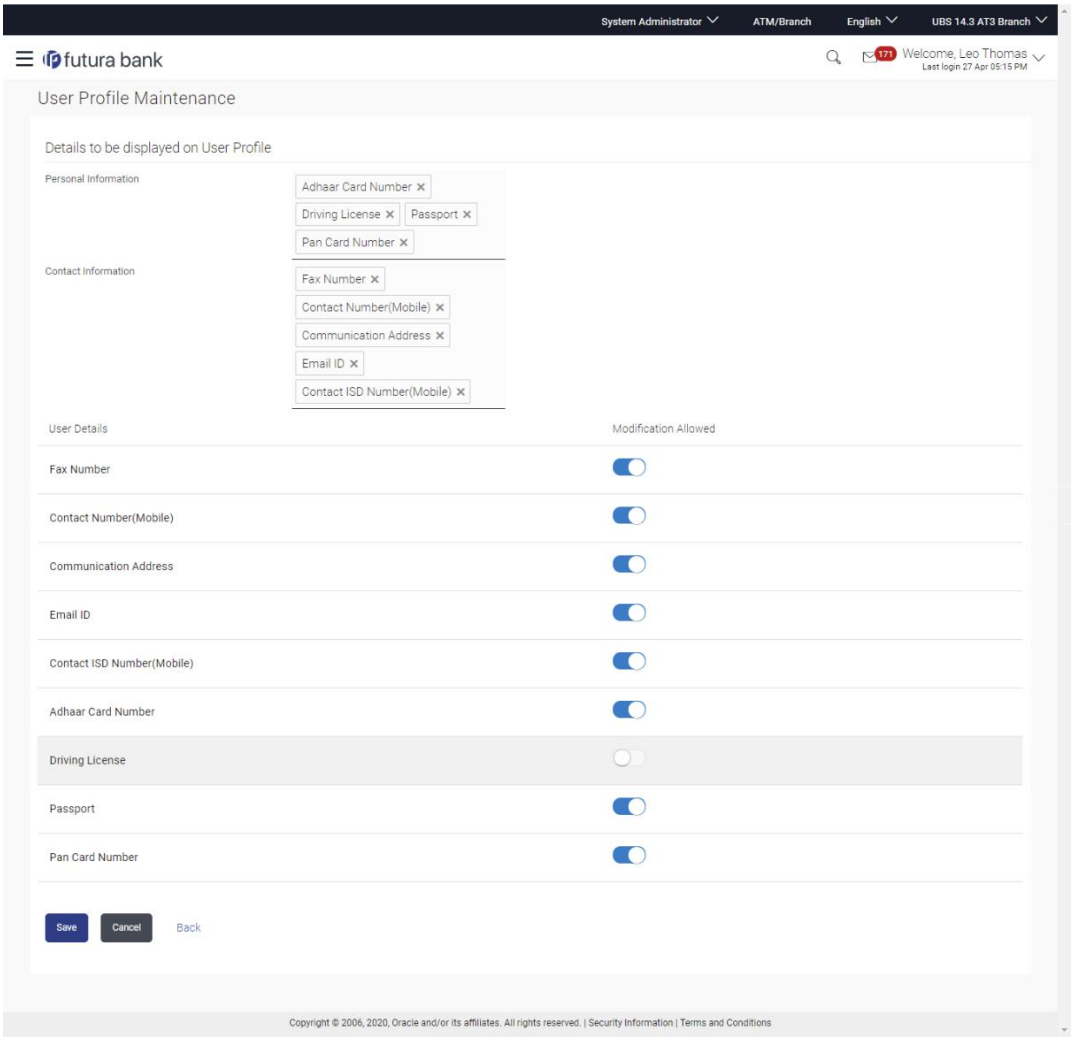
29.2 User Profile - Edit

This function enables the bank/system administrator to modify the existing setup done for user profile details.

To modify user profile details:

1. Navigate to the **User Profile Maintenance** screen, if the user profile is already maintained for user, appears on **User Profile Maintenance- View** screen.
2. Click **Edit** to modify the user profile details. The **User Profile Maintenance - Edit** screen appears with the details.
   OR
   Click **Cancel** to cancel the transaction.

User Profile Maintenance- Edit



3. Modify the required details, e.g. date of birth, PAN number, Aadhar number, passport number communication address and phone number, fax number etc.
4. Click **Save** to save the user profile details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
5. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Edit** to modify the user profile details.
6. The success message of user profile maintenance completed successfully appears along with the transaction reference number and status.

FAQ

5. **Can this maintenance be done for Corporate and Admin users as well?**

   No, this maintenance can only be done for Retail users.

6. **Can the System/bank administrator select any value from the personal /contact information field and the same will start appearing on the business user's profile screen?**

   Yes, the values selected by Bank administrator will be displayed to business user in his/her profile, provided those fields are supported by host system.

30. Payee Restriction Setup

Bank customers add payees or beneficiaries to transfer funds from one account to another. Bank can limit the number of payees that can be added by the retail user in a day.

Payee Restriction set up maintenance allows the System Administrator to restrict the number of payees that a retail user can create for each payment network per day.

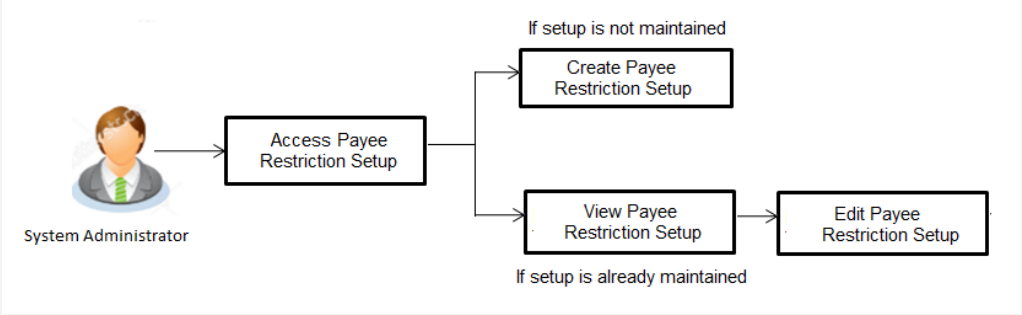
System Administrator can also restrict the total number of payees irrespective of payment network that the retail user can create per day.

Payee restriction setup can be done for a User type and also for a User type and Segment combination.

Prerequisites:

- Transaction access is provided to System Administrator
- Approval rule set up for System Administrator to perform the actions

Workflow



Features supported in Application

Payee Restriction Setup maintenance is created only once at the 'Day 1' configuration by the System Administrator. However it can later be viewed and modified.

This option allows an administrator to:

- Create Payee Restriction Maintenance
- View Existing Maintenance
- Edit Maintenance

How to reach here:

System Administrator Dashboard > Payments > Payee Restrictions
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Payments > Payee Restrictions
OR
Search Bar > Payments - Payee Restrictions

30.1 Payee Restriction Setup - View

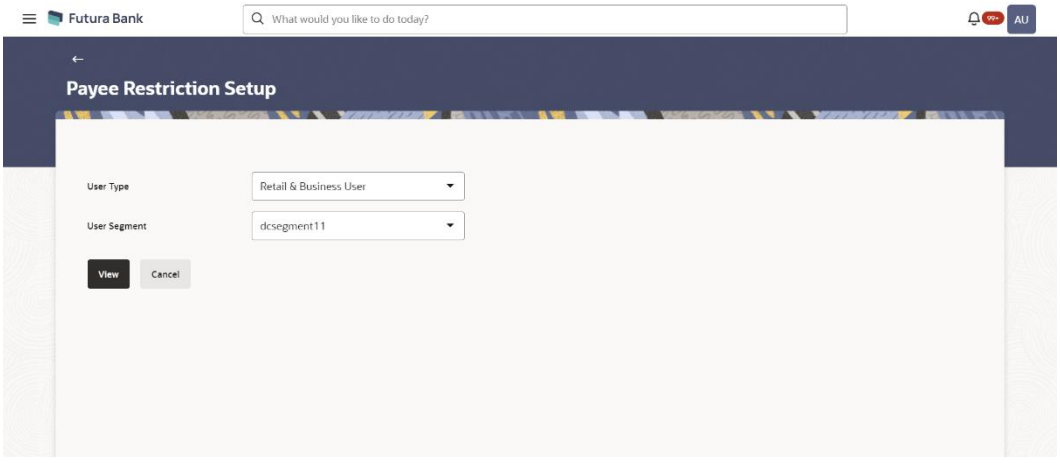
Using this option, administrator can search for particular payee restriction set up based on different search parameters. The search results displays a payee restriction set up based on search filters selected.

System displays the payee restriction set up for the search criteria entered. When System Administrator user is accessing Payee Restriction Set-up for the very first time, the limit set up for payment network type is defaulted to 'No'.

To view payee restriction setup:

1. From the **User Type** list, select the appropriate user whose payee restriction setup to be viewed.
2. From the **User Segment** list, select the appropriate name of segment whose payee restriction setup to be viewed.
3. Click **View**. The **Payee Restriction Setup** screen with payee restriction setup appears.
   OR
   Click **Cancel** to cancel the process.

Payee Restriction Setup

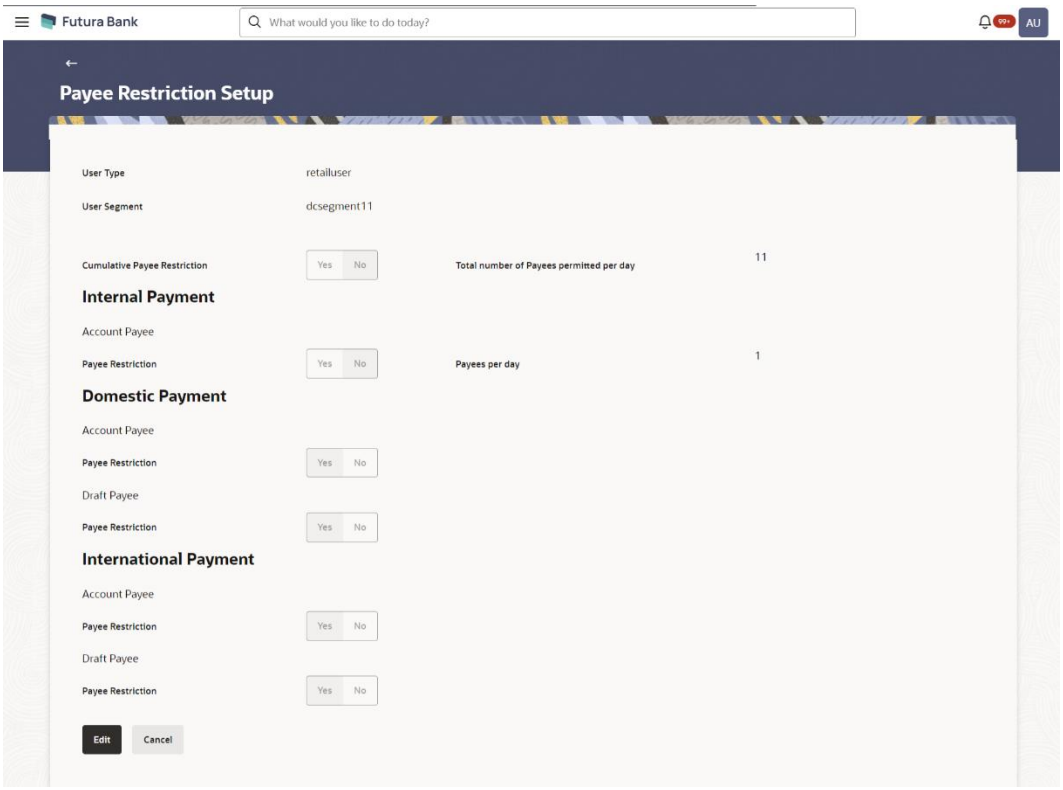


Field Description

Field Name	Description
User Type	Select the user type for which payee restriction setup details needs to be searched.

Field Name	Description
User Segment	Select the name of segment or which payee restriction setup details needs to be searched.

Payee Restriction Setup



Field Description

Field Name	Description
User Type	The user type for which payee restriction setup is done.
User Segment	The user segment for which payee restriction setup is done.
Cumulative Payee Restriction	Whether the cumulative payee restriction is enabled or not.
Total number of Payees permitted per day	Displays the total number of payees that are permitted, if the cumulative payee restriction is enabled.

Field Name	Description
Internal Payment	
Account Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for internal payment.
Payees Per Day	Displays the total number of payees that are permitted, if the account payee restriction for internal payment is enabled.
Domestic Payment	
Account Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for domestic payment. For India region this will be applicable for all the payments falling under domestic type of payment (NEFT, RTGS and IMPS).
Payees Per day	Displays the total number of payees that are permitted, if the account payee restriction for internal payment is enabled.
Draft Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for a domestic draft payment.
Payees Per Day	Displays the total number of payees that are permitted, if the account payee restriction for internal payment is enabled.
International Payment	
Account Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for international payment.
Payees Per Day	Displays the total number of payees that are permitted, if the account payee restriction for international payment is enabled.
Draft Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for international draft payment.
Payees Per Day	Displays the total number of payees that are permitted, if the account payee restriction for international draft payment is enabled.

4. Click **Edit** to edit the payee restriction set up.
   The **Payee Restriction Set-up-Edit** screen with values in editable form appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.

30.2 Payee Restriction Setup - Edit

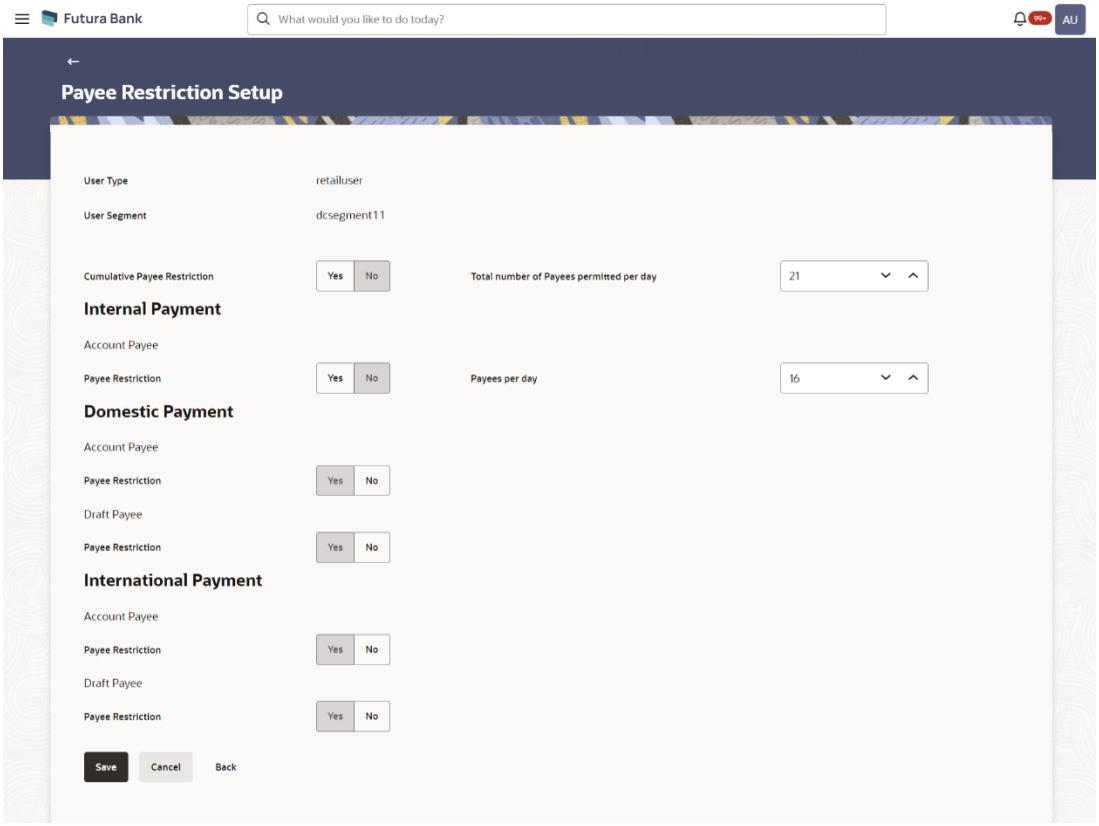
System Administrator can modify existing payee restriction maintenance.

Using this option, System Administrator can edit the payee restriction option for a specific payment network. Also an edit is permitted on number of payees per payment network and for cumulative combined limit irrespective of payment network.

To edit a payee restriction setup:

1. Navigate to the **Payee Restriction Setup – View** screen.
2. Click **Edit**. The **Payee Restriction Setup - Edit** screen appears.

Payee Restriction Setup - Edit



Field Description

Field Name	Description
User Type	The user type for which payee restriction setup is done.

Field Name	Description
User Segment	The user segment for which payee restriction setup is done.
Cumulative Payee Restriction	Whether the cumulative payee restriction is enabled or not. This field is not editable.
Total number of Payees permitted per day	Displays the total number of payees that are permitted, if the cumulative payee restriction is enabled. This field will only be displayed if cumulative payee restriction is enabled.
Internal Payment	
Account Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for internal payment. For India region this will be applicable for all the payments falling under domestic type of payment (NEFT, RTGS and IMPS).
Payees Per Day	Displays the total number of payees that are permitted, if the account payee restriction for internal payment is enabled. Field will not be displayed if Account - Payee Restriction for Internal Payment is disabled.
Domestic Payment	
Account Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for domestic payment.
Draft Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for a domestic draft payment.
Payees Per Day	Displays the total number of payees that are permitted, if the account payee restriction for internal payment is enabled. Field will not be displayed if Draft - Payee Restriction for Domestic Payment is disabled.
International Payment	
Account Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for international payment.

Field Name	Description
Payees Per Day	Displays the total number of payees that are permitted, if the account payee restriction for international payment is enabled. Field will not be displayed if International Payment - Payee Restriction for Domestic Payment is disabled.
Draft Payee - Payee Restriction	Whether the account payee restriction is enabled or not, for international draft payment.
Payees Per Day	Displays the total number of payees that are permitted, if the account payee restriction for international draft payment is enabled. Field will not be displayed if International Draft - Payee Restriction for Domestic Payment is disabled.

3. In the **Cumulative Payee Restriction/ Account Payee - Payee Restriction/ Draft Payee - Payee Restriction** field, select the appropriate option.
   a. If user select **Yes** option:
      i. Edit the values in **Total number of Payees permitted per day** field.
      OR
      Click or to edit the values.
   b. If user select **No** option:
      i. Fields Total Number of payees per day and Payees per day are not displayed for respective payment type.
4. Select the transactions whose details you want to edit.
5. Click **Save** to save the changes made to the payee restriction set up. The message box informing that the changes will be effective next day appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate back to previous screen.
6. The **Payee Restriction Set-up – Edit – Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation.

   OR
   Click **Back** to navigate back to previous screen.
7. The success message of Payee Restriction Set-up – Edit appears along with the transaction reference number.
8. Click **OK** to complete the transaction and navigate back to 'Dashboard'.

30.3 Payee Restriction Setup - Create

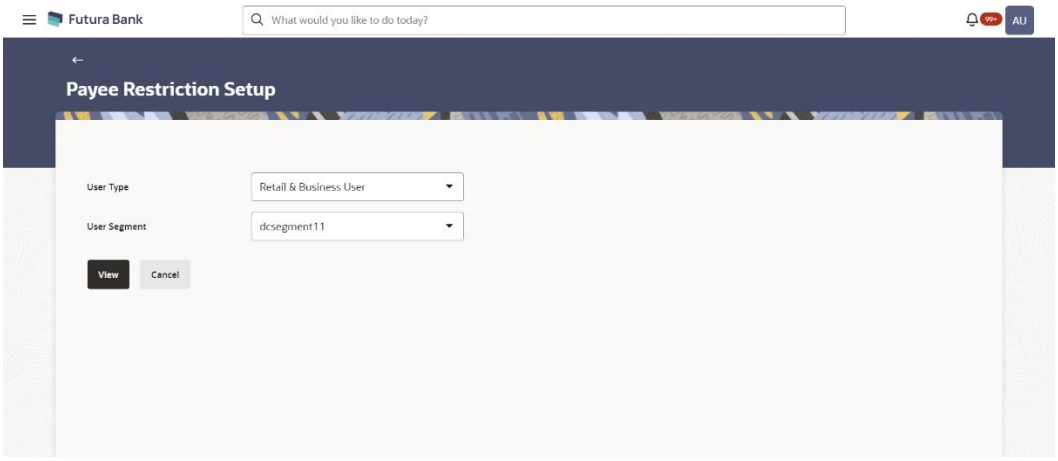
System Administrator can setup Payee Restriction at the 'Day 1' configuration for a user type or a user type and user segment combination.

Using this option, System Administrator can setup payee restriction for a specific payment network. Administrator can also define permitted number of payees per payment network along with the cumulative combined limit for the number of payees irrespective of payment network.

To create payee restriction setup:

1. From **User Type** list, select appropriate user for whom payee restriction setup is to be done.
2. From the **User Segment** list, select appropriate user segment for whom payee restriction setup is to be done.
3. Click **View**. The popup message of Payee Restriction Setup for the selected segment not done appears.

Payee Restriction Setup screen

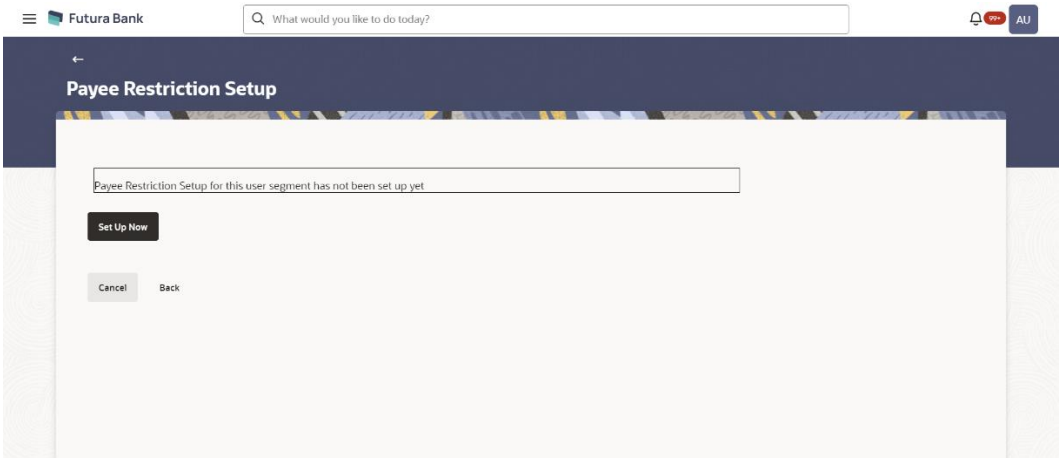


Field Description

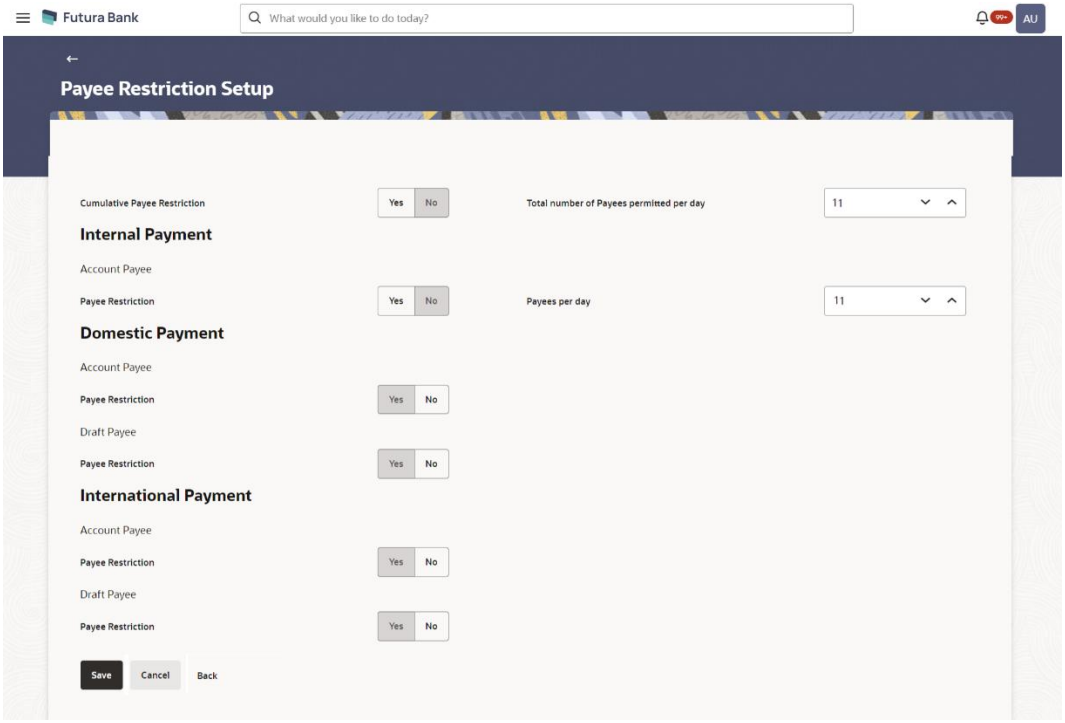
Field Name	Description
User Type	The user type for which payee restriction setup is done.
User Segment	The user segment for which payee restriction setup is done.

4. Click **Set Up Now** to create Payee Restriction Setup. **Payee Restriction Setup - Create** screen appears.
   OR
   Click **Cancel** to cancel the operation.
   OR
   Click **Back** to navigate back to previous screen.

Payee Restriction Setup screen



Payee Restriction Setup - Create



Field Description

Field Name	Description
Cumulative Payee Restriction	Enable cumulative payee restriction to define the total number of payees across the network types

Field Name	Description
Total number of Payees permitted per day	Specify the total number of payees that are permitted, if the cumulative payee restriction is enabled. This field will only be displayed if cumulative payee restriction is enabled.
Internal Payment	
Account Payee - Payee Restriction	Enable cumulative payee restriction to define the number of payees for internal payment. For India region this will be applicable for all the payments falling under domestic type of payment (NEFT, RTGS and IMPS).
Payees Per Day	Specify the total number of payees that are permitted, if the account payee restriction for internal payment is enabled. Field will not be displayed if Account - Payee Restriction for Internal Payment is disabled.
Domestic Payment	
Account Payee - Payee Restriction	Enable cumulative payee restriction to define the number of payees for domestic payment.
Payees Per Day	Specify the total number of payees that are permitted, if the account payee restriction for internal payment is enabled. Field will not be displayed if Account Payee Restriction for Domestic Payment is disabled.
Draft Payee - Payee Restriction	Enable cumulative payee restriction to define the number of payees for a domestic draft payment.
Payees Per Day	Specify the total number of payees that are permitted, if the account payee restriction for internal payment is enabled. Field will not be displayed if Draft - Payee Restriction for Domestic Payment is disabled.
International Payment	
Account Payee - Payee Restriction	Enable cumulative payee restriction to define the number of payees for international payment.

Field Name	Description
Payees Per Day	Specify the total number of payees that are permitted, if the account payee restriction for international payment is enabled. Field will not be displayed if International Payment - Payee Restriction for Domestic Payment is disabled.
Draft Payee - Payee Restriction	Enable cumulative payee restriction to define the number of payees for international draft payment.
Payees Per Day	Specify the total number of payees that are permitted, if the account payee restriction for international draft payment is enabled. Field will not be displayed if International Draft - Payee Restriction for Domestic Payment is disabled.

5. In the **Cumulative Payee Restriction/ Account Payee - Payee Restriction/ Draft Payee - Payee Restriction** field, select the appropriate option.
   a. If user select **Yes** option:
      i. Update the values for the **Total number of Payees permitted per day** or **Payees Per Day** fields.
      OR
      Click or to increase or decrease the values.
   b. If user select **No** option:
      i. Fields **Total Number of payees per day** and **Payees per day** are not displayed for respective payment type.
6. Select the transactions whose details you want to define.
7. Click **Save** to save the changes made to the payee restriction set up. The message box informing that the changes will be effective next day appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate back to previous screen.
8. The **Payee Restriction Set-up– Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation.
   OR
   Click **Back** to navigate back to previous screen.
9. The success message of Payee Restriction Set-up creation appears along with the transaction reference number. Click **OK** to complete the transaction and navigate back to 'Dashboard'.

FAQ

1. **Will edited maintenance be applicable from immediate effect?**

   No, edited maintenance will be applicable from next calendar date.

2. **What happens if the user's cumulative payee limit for a day is fully utilized but network for which he is creating a payee is available?**

   System will first check the availability of cumulative payee limit. If available, will check network level payee availability limit. If both the conditions are met, user is allowed to create a payee.

3. **Is this maintenance is also applicable for corporate type of users?**

   No, currently this maintenance is applicable only to Retail Users.

31. Forex Deal Maintenance

Using this option System Administrator can maintain currency pair. The maintained currency pairs are made available to corporate users to book deals and utilize those while making payments.

Features supported in application

Using this option System Administrator can perform the following actions:

- Maintain currency Pair

How to reach here:

System Administrator Dashboard > Payments > Forex Deal Maintenance
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Payments > Forex Deal Maintenance

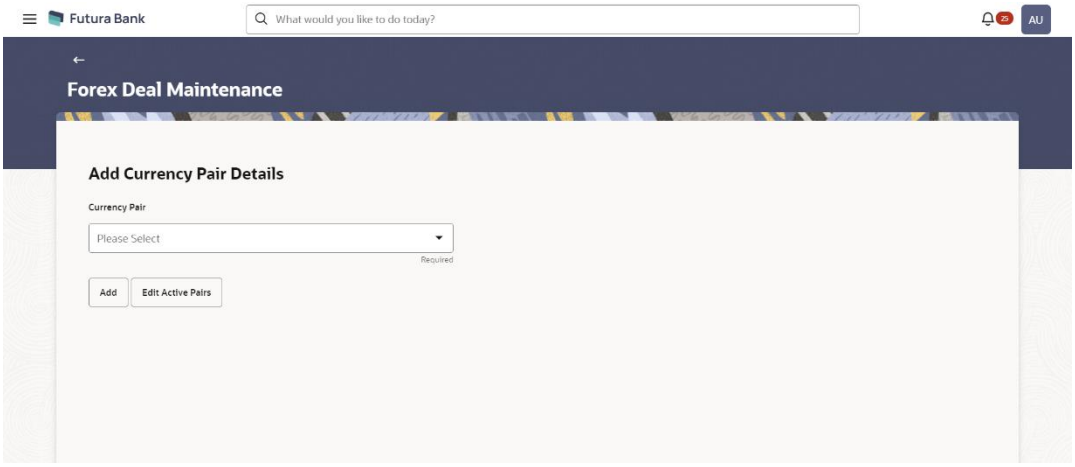
31.1 Add Currency Pairs

Using this option System Administrator can define currency pairs.

To add currency pair:

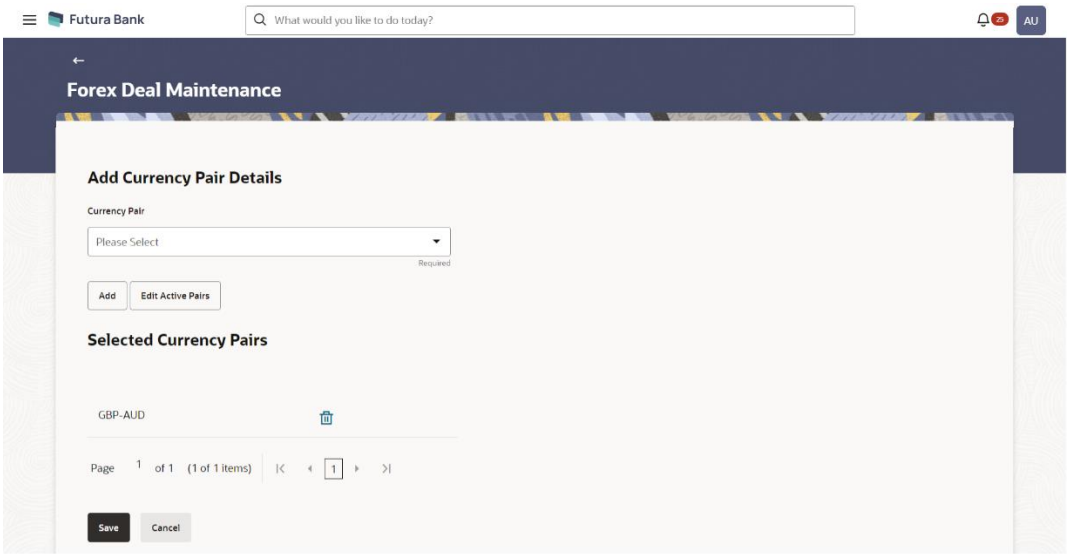
1. From the **Currency Pair** list, select the appropriate currency pair.

Forex Deal Maintenance – Add Currency Pair



2. Click **Add** to add the currency pair.

Forex Deal Maintenance - Create



Field Description

Field Name	Description
Add Currency Pair Details	
Currency Pair	List of the permissible currency combinations in which corporate user can book a deal.
Selected Currency Pairs	
Currency Pair	The maintained currency pair for corporate users.
Action	Allows user to maintain i.e. delete the selected currency pairs.

3. The Currency pair gets added in the **Selected Currency Pairs** section.
4. Click to delete the added currency pair.
5. Click **Save** to save the changes.
   OR
   Click **Cancel** to cancel the transaction.
6. The **Forex Deal Maintenance - Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation.

   OR
   Click **Back** to navigate back to previous screen.

7. The success message of Forex Deal Maintenance appears along with the transaction reference number.
8. Click **OK** to complete the transaction and navigate back to ‘Dashboard’.

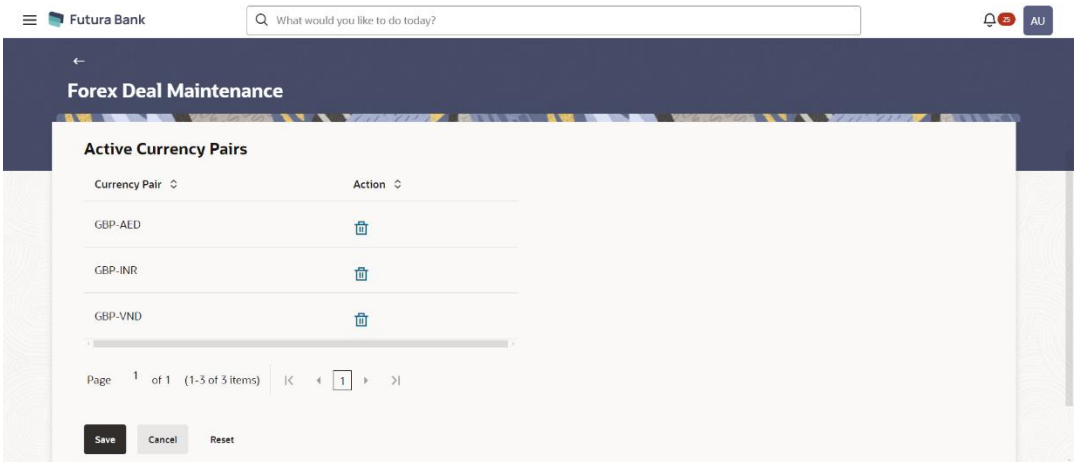
31.2 Update Forex Deal

Using this option, System Administrator can modify active currency pairs maintained in the application. System Administrator can delete the existing maintained currency pair.

To update forex deal:

1. Click **Edit Active Pairs**.
   The list of active currency pairs maintained in application appears.

Forex Deal Maintenance- Edit



Field Description

Field Name	Description
Active Currency Pairs	
Action	Allows user to maintain i.e. delete the existing currency pairs.

2. Click to delete the selected currency pair.
3. Click **Save** to save the changes.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Reset** to clear the entered details.

4. The **Forex Deal Maintenance - Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation.

   OR
   Click **Back** to navigate back to previous screen.
5. The success message of Forex Deal Maintenance appears along with the transaction reference number.
6. Click **OK** to complete the transaction and navigate back to ‘Dashboard’.

32. Touch Point Maintenance

Touch points are different channels/medium through which transactions or inquiries can be performed in OBDX.

Touch points in OBDX are of type ‘Internal’ and ‘External’.

Internal Touch points are defined as part of Day 0 definition whereas External Touch Points are typically third party applications that can be defined by the System Administrator as part of onboarding in OBDX.

Internal Touch Points defined/available as parts of OBDX system are as follows:

- Internet
- Mobile App
- Mobile Browser
- SMS
- Missed Call
- Siri/Chatbot
- Snapshot
- Wearables

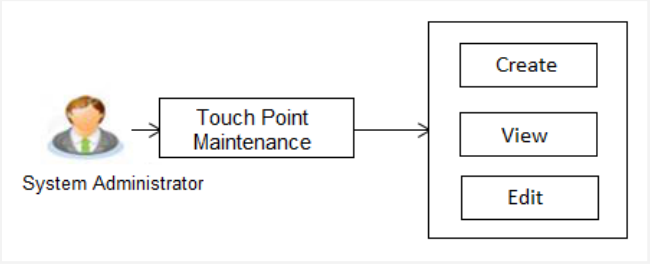
External Touch Points enable the user to perform inquiries and transactions from Third Party applications provided the user has provided consent to the Third Party Application. Each Third Party application i.e. Client defined on the OAuth Server is onboarded as an External Touch Point.

As part of Touch Point Maintenance, Touch Points can be defined/created, viewed/inquired and modified by the System Administrator

Prerequisites

- Transaction Access has been provided to the System Administrator
- Approval Rules have been setup for approval of Touch Point Maintenance

Workflow



Features supported in application

The administrator can perform the following actions:

- Search/ View Touch Point
- Create Touch Point
- Edit Touch Point

How to reach here:

System Administrator Dashboard > Authorization and Access Controls >Touch Points
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Authorization and Access Controls >Touch Points

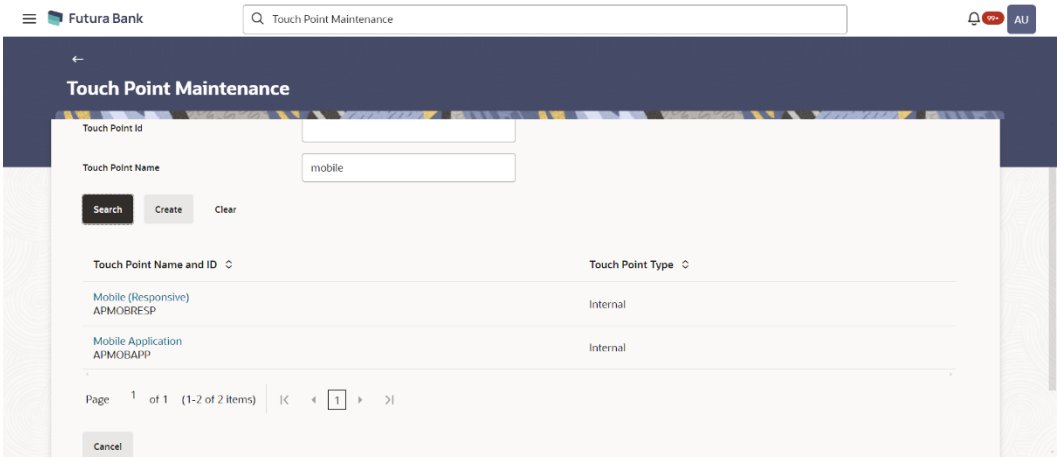
32.1 Touch Point Maintenance - View

Using this option, System Administrator can search and view details for specific touch point based on different search parameters like Touch Point ID or Touch Point name.

To search and view touch point:

1. In the **Touch Point Maintenance** screen, enter the search parameters and click **Search**. The **Touch Point Maintenance** screen with search results appears based on the search criteria.
   OR
   Click **Cancel** if you want to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.

Touch Point Maintenance - Search

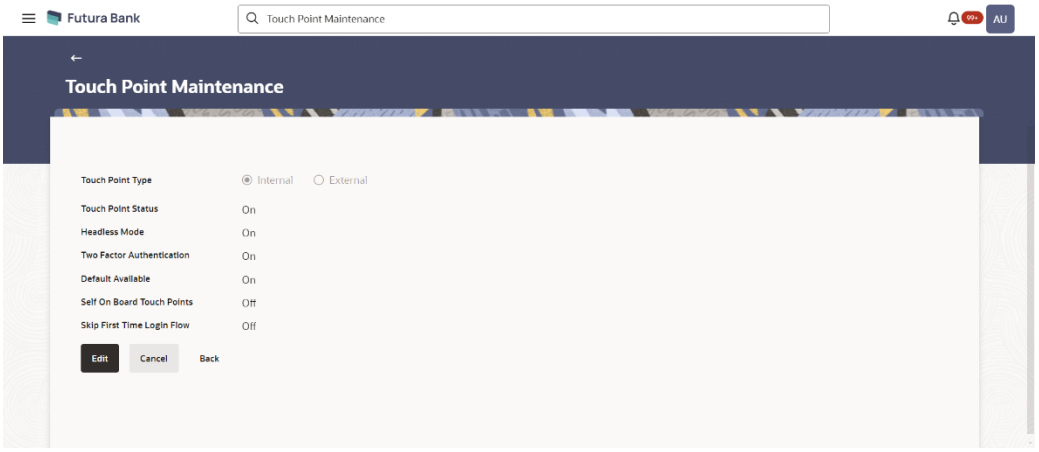


Field Description

Field Name	Description
Touch Point ID	Specify the touch point ID to search a specific Touch point by ID.
Touch Point Name	Specify the touch point name to search a Touch point by name.
Search Results	
Touch Point Name and ID	Displays the touch point name and unique ID defined for a Touch point.
Touch Point Type	Displays the touch point type i.e. internal/ external against the Touch points.

2. Click the **Touch Point Name and ID** link to view details of the touch point. The **Touch Point Maintenance - View** screen appears.

Touch Point Maintenance - View



Field Description

Field Name	Description
Touch Point ID	Unique ID defined for the Touch Point.
Touch Point Name	Name of the touch point.
Touch Point Type	Type of touch point i.e. whether touch point is of type internal or external.

Field Name	Description
Client ID	Client ID of the touch point if touch point is of type internal or external.
Scope	The applicable scope(s) defined for touch point in case of type **External**.
Upload Logo	The logo of the Third Party. This field is displayed if the **Touch Point Type** is **External**.
Touch Point Status	Status of the Touch Point i.e. whether it is Inactive or Active. If touch point is marked as Inactive, then the system will not honor the request i.e. transaction or inquiry is initiated from that touch point.
Headless Mode	Mode in which the touch point operates i.e. headless mode enabled / disabled. If headless mode is enabled, it means the touch point is capable of working without user interface and session parameters **Note:** By default, the mode is in disabled state.
Two Factor Authentication	Two Factor Authentication enabled / disabled for the touch point.
Default Available	Touch point default available to users. If enabled, then the user gets access to touch points which are default available.
Self On Board Touch Points	Whether the user can self on board himself on the touch point or by bank administrator.
Skip First Time Login Flow	Displays if Skip First Time Login Flow option is checked by the user. If this option is enabled for the selected touch point, user will not be shown the first time login steps (configured in system rule), when he/she logs in for the first time.
Consent Required	To decide if Consent definition and validation is required for a Touch Point i.e. TPPs. For UK/Berlin Open Banking, it should always be defined as 'Y'.

3. Click **Edit** to modify touch point details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.

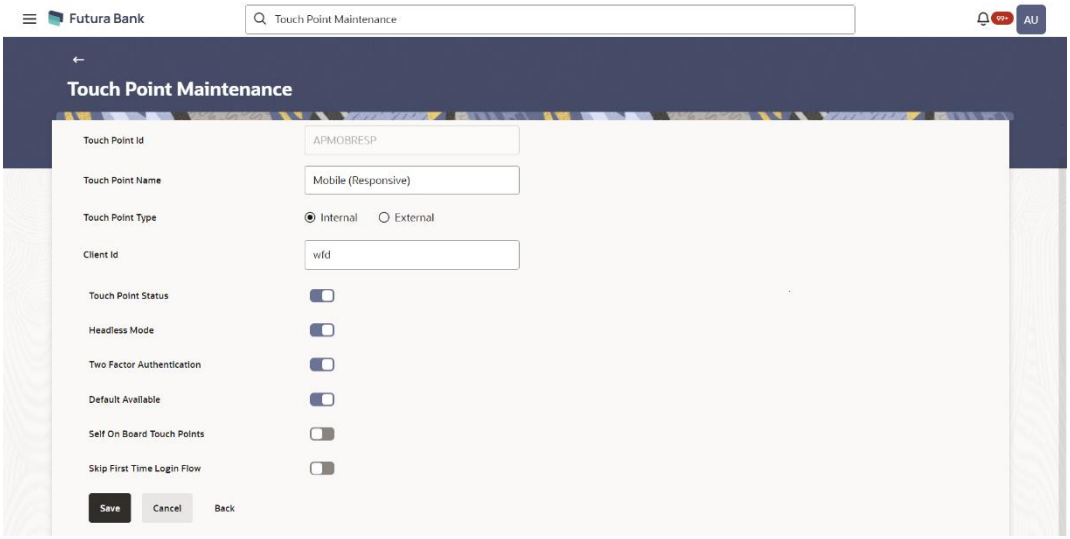
32.2 Touch Point Maintenance - Edit

Using this option, System Administrator can modify the details of a touch point

To modify touch point details:

1. In the **Touch Point Maintenance** screen, enter the search parameters and click **Search**. The **Touch Point Maintenance** screen with search results appears based on the search criteria.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
2. Click the **Touch Point Name and ID** link to view details of the touch point. The **Touch Point Maintenance - View** screen appears.
3. Click **Edit** to modify the touch point details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.

Touch Point Maintenance - Edit



Field Description

Field Name	Description
Touch Point ID	Displays the Unique ID for the Touch Point and cannot be modified.
Touch Point Name	Displays the name of the touch point. The same can be modified.

Field Name	Description
Touch Point Type	Displays the type of touch point i.e. whether touch point is of type internal or external. The same can be modified
Client ID	Displays the Client ID of the touch point if touch point is of type External. The same can be modified. This field is mandatory for External type of touch point.
Scope	Displays the applicable scope(s) defined for touch point in case of type External. The same can be modified i.e. new scopes can be added and/or existing can be removed.
Upload Logo	The logo of the Third Party. This field is displayed if the **Touch Point Type** is **External**.
Touch Point Status	Displays the status of touch point. The same can be modified to enable to an active state or disable to make it inactive.
Headless Mode	Displays the mode in which the touch point operates i.e. headless mode enabled / disabled. The same can be modified to enable/disable the mode
Two Factor Authentication	Displays if Two Factor Authentication is enabled/disabled for the touch point. The same can be modified.
Default Available	Displays if Touch point is available to users by default. If enabled, then the user gets access to touch points which are default available.
Self On Board Touch Points	Displays if Touch point can be on boarded by the user. The same can be modified.
Skip First Time Login Flow	Displays if Skip First Time Login Flow option is checked by the user. If this option is enabled for the selected touch point, user will not be shown the first time login steps (configured in system rule), when he/she logs in for the first time. The same can be modified.
Consent Required	To decide if Consent definition and validation is required for a Touch Point i.e. TPPs. For UK/Berlin Open Banking, it should always be defined as 'Y'. The same can be modified.

4. Modify the required details, e.g. Touch Point Name, Touch Point Type, Client ID, Scope, Logo, Touch Point Status, Headless Mode, Two Factor Authentication, Default Available and Self On board Touch Points.
5. Click **Save** to save the touch point details.
   OR
   Click **Cancel** to cancel the transaction.

OR
Click **Back** to navigate back to previous screen.

6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
7. The success message of Touch Point Maintenance saved successfully appears along with the transaction reference number.
   Click **OK** to complete the transaction.

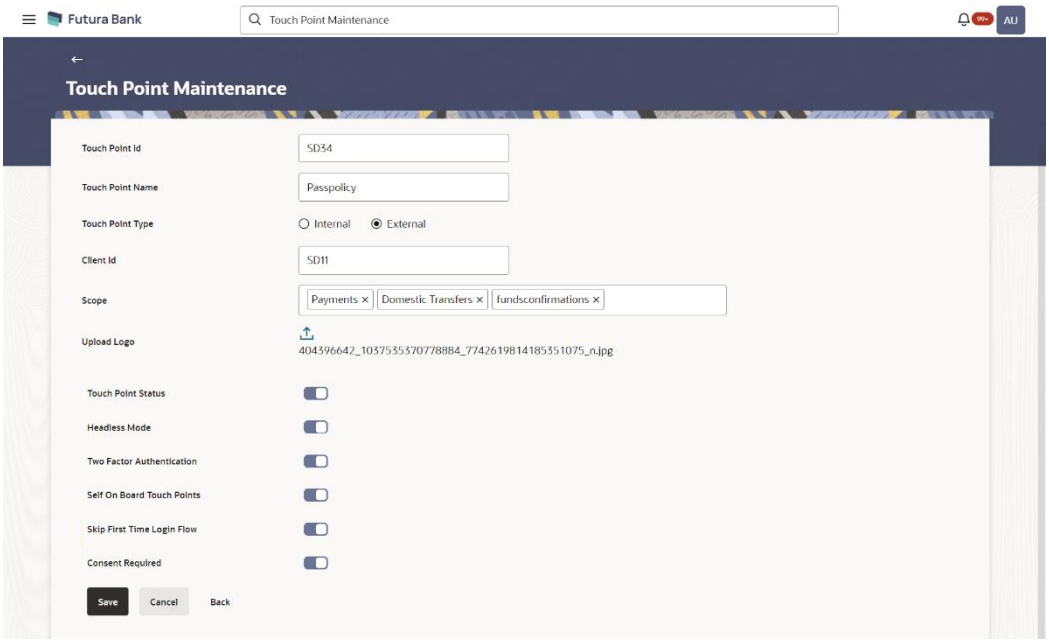
32.3 Touch Point Maintenance - Create

Using this option, System Administrator can create new touch point of type Internal or External

To create a touch point:

1. In the **Touch Point Maintenance** screen, click **Create**. The **Touch Point Maintenance - Create** screen appears.

Touch Point Maintenance - Create



Field Description

Field Name	Description
Touch Point ID	Specify the unique ID for the Touch Point.

Field Name	Description
Touch Point Name	Specify the name for the Touch Point.
Touch Point Type	Select the type of Touch point type i.e. whether the type is Internal or External
Client ID	Specify the Client ID for the touch point. This field is mandatory for External Type of Touch point.
Scope	Specify the applicable scope(s) for the touch point. This field is enabled, if you select **External** option in the **Touch Point Type** field.
Upload Logo	Upload logo of the Third Party Provider through browse and upload image option. This field is enabled, if you select **External** option in the **Touch Point Type** field.
Touch Point Status	Select the status for the touch point i.e. whether it is active/inactive.
Headless Mode	Select the mode in which the touch point operates i.e. whether headless mode is to be enabled for a touch point. **Note:** By default this mode is in disabled state.
Two Factor Authentication	Select if Two Factor Authentication is required for a touch point.
Default Available	Select if Touch point is to be default made available to users. If enabled, then the user gets access to touch points which are default available
Self On Board Touch Points	Select if user will self on board himself on the touch point or by the bank administrator. If the bank administrator on boards the user on a touch point, then the same needs to be disabled.
Skip First Time Login Flow	Select if user wants to skip the first time login flow for a touch point. If this option is enabled for the selected touch point, user will not be shown the first time login steps (configured in system rule), when he/she logs in for the first time.
Consent Required	Select if user wants Consent definition and validation is required for a Touch Point i.e. TPPs. For UK/Berlin Open Banking, it should always be defined as 'Y'.

2. In the **Touch Point ID** field, enter the unique ID for the touch point.

3. In the **Touch Point Name** field, enter the name for touch point.
4. In the **Touch Point Type** field, select the appropriate option i.e. Internal or External.
5. In the Client ID field, enter the client ID
   a. If you select **External**;
      i. Click **Scope**; select the appropriate scope from the drop-down.
      ii. Click on upload icon to upload a logo for the external type of touch point.
6. Click the **Touch Point Status** toggle to enable it to mark the touch point 'Active'.
7. Click the **Headless Mode** toggle to enable the touch point in headless mode.
8. Click the **Two Factor Authentication** toggle to enable 2FA for a touch point.
9. Click the **Default Available** toggle to make the touch point available to users by default in case of self-onboarding.
10. Click the **Self On board Touch Point** toggle if the user will self-onboard himself on the touch point and not by bank administrator.
11. Click the **Skip First Time Login Flow** toggle if the user wants to skip it for touch point.
12. Click **Save** to save the Touch Point details.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate back to previous screen.
13. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate back to previous screen.
14. The success message of touch point creation successfully appears along with the transaction reference number.
    Click **OK** to complete the transaction.

33. Touch Point Group Maintenance

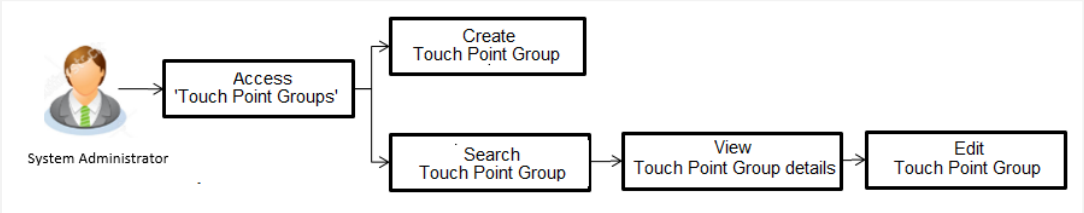
Touch points are different channels e.g. Internet, Mobile, SMS, Third Party applications etc. through which the OBDX services can be accessed. This maintenance enables the System Administrator user to group two or multiple touch points together for the purpose of defining common limits for a transaction accessed from any Touch point grouped together.

Further this maintenance facilitates user to view and modify the touch point groups.

Prerequisites

- Transaction access is provided to system administrator.
- Approval rule set up for system administrator to perform the actions.
- Multiple touch points are maintained.

Workflow



Features supported in application

The administrator can perform the following actions:

- Create Touch Point Groups
- Search/ View Touch Point Groups
- Edit Touch Point Groups

How to reach here:

System Administrator Dashboard > Authorization and Access Controls >Touch Point Groups
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Authorization and Access Controls > Touch Point Groups

33.1 Touch Point Group Maintenance - View

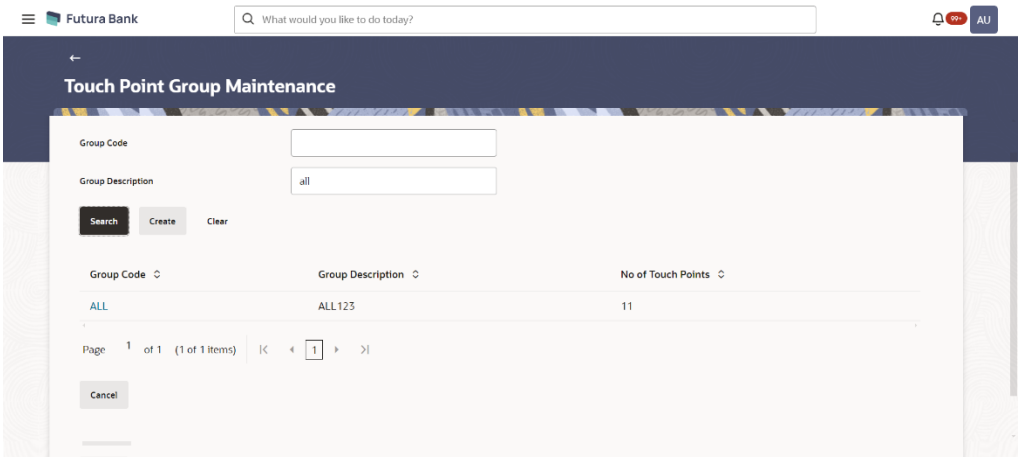
Using this option, System Administrator can search and view details for particular touch point groups based on different search parameters like group code and/or group description.

To search and view touch point group:

1. In the **Touch Point Group Maintenance** screen, enter the search parameters and click **Search**.

The **Touch Point Group Maintenance** screen with search results appears based on the search criteria.
OR
Click **Cancel** to cancel the search process.
OR
Click **Clear** to reset the search parameters.

Touch Point Group Maintenance - Search

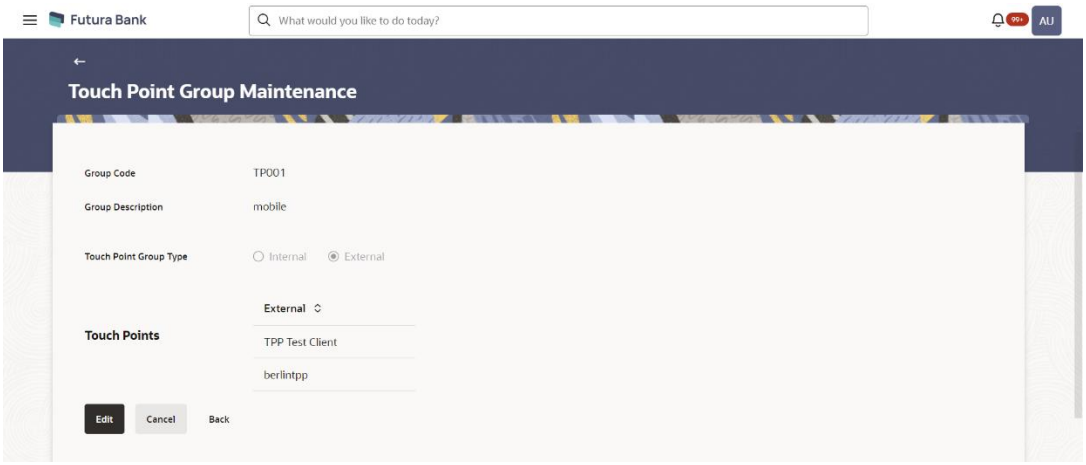


Field Description

Field Name	Description
Group Code	Search the touch point groups with group code.
Group Description	Search the touch point groups with group description.
Search Results	
Group Code	Displays the group code defined for Touch Point Groups.
Group Description	Displays the group description defined for Touch Point Group.
No of Touch Points	Displays the number of touch points associated with the touch point groups.

2. Click the **Group Code** link to view the touch point group details. The **Touch Point Group Maintenance - View** screen appears.

Touch Point Group Maintenance - View



Field Description

Field Name	Description
Group Code	Group code defined for touch point group.
Group Description	Group description defined for touch point groups.
Touch Point Group Type	Type of touch point group i.e. whether touch point group type is internal or external.
Internal Touch Points	Displays internal touch points which are part of touch point group in disable mode.
External Touch Points	Displays external touch points which are part of touch point group in disable mode.

3. Click **Edit** to add or remove the touch points from the touch point group.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.

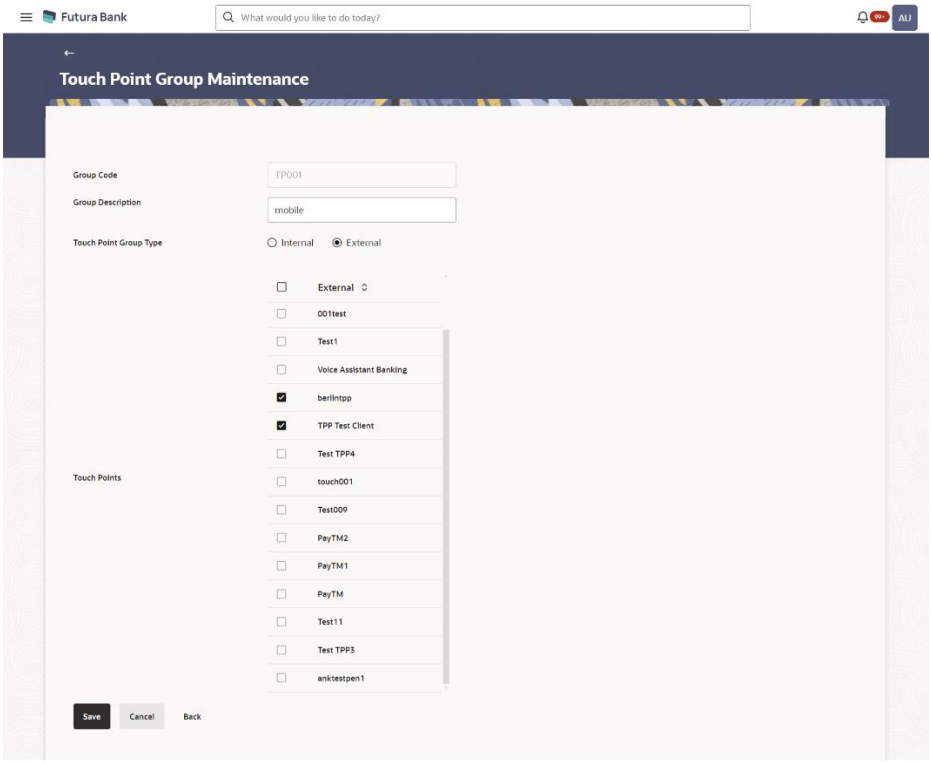
33.2 Touch Point Group Maintenance - Edit

Using this option, System Administrator can add or remove the touch points from the touch point group. Clubbing of touch points as a part of multiple groups is not allowed. Touch points already grouped as a part of other groups will not be available for selection.

To modify touch point group:

1. In the **Touch Point Group Maintenance** screen, enter the search parameters and click **Search**.
   The **Touch Point Group Maintenance** screen with search results appears based on the search criteria.
   OR
   Click **Cancel** to cancel the search process.
   OR
   Click **Clear** to reset the search parameters.
2. Click the **Group Code** link to view the touch point group details. The **Touch Point Group Maintenance - View** screen appears.
3. Click **Edit** the **Touch Point Group Maintenance - Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.

Touch Point Group Maintenance - Edit



Field Description

Field Name	Description
Group Code	Group code defined for touch point group.
Group Description	Group description defined for touch point groups.
Touch Point Group Type	Displays the type of touch point group i.e. whether touch point group is of type internal or external. The same can be modified.
Touch Points	
Internal Touch Points	Displays all the internal touch points. Touch points which are the part of a group will be shown as pre-selected. **Note:** 1) User can de-select a pre-selected internal touch points which are already part of the group. 2) Other Internal touch points which are not part of any other group will be listed for selection. 3) The touch points which are already a part of one of the groups will be shown in disable mode. (one Touch point can be part of on group only)
External Touch Points	Displays all the external touch points. Touch points which are the part of a group will be shown as pre-selected. **Note:** 1) User can de-select an external touch points which are already part of a group will be shown as pre-selected. 2) Other external touch points which are not part of any other group will be listed for selection. 3) The touch points which are already a part of one of the group will be shown in disable mode.

4. Modify the required details, e.g. Group Description, Internal / External Touch Points.
5. Click **Save** to save the touch point group details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.

7. The success message of Touch Point Group Maintenance saved successfully appears along with the transaction reference number.
   Click **OK** to complete the transaction.

33.3 Touch Point Group Maintenance - Create

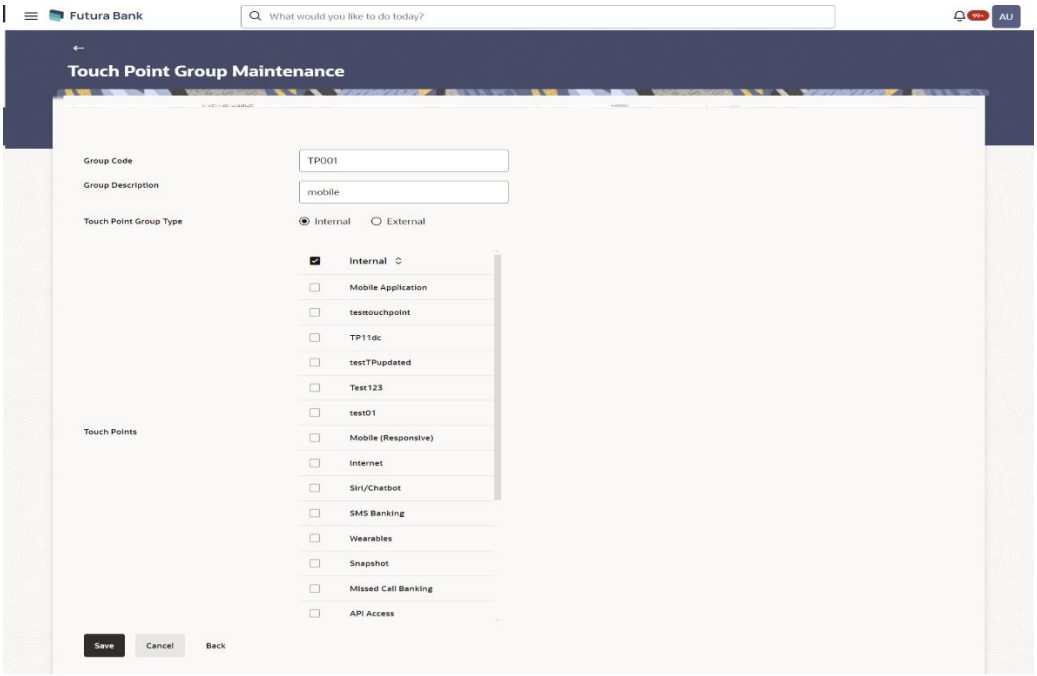
Using this option, System Administrator can create a new touch point group and add touch points to a group.

Note: System Administrator cannot club one touch point as part of multiple groups. While creating group, touch points which are already part of a group will not be available for selection.

To create a touch point group:

1. In the **Touch Point Group Maintenance** screen, click **Create**. The **Touch Point Group Maintenance - Create** screen appears.

Touch Point Group Maintenance - Create



Field Description

Field Name	Description
Group Code	Unique group code defined for touch point group.

Field Name	Description
Group Description	Touch point group description defined for touch point groups.
Touch Point Group Type	Select the type of Touch point group type i.e. whether the type is Internal or External.
Touch Points	
Internal Touch Points	Displays all the internal touch points maintained. **Note:** 1) Internal touch points which are not part of any other group will be listed for selection. 2) Touch points which are already a part of any other group will be shown in disabled mode.
External Touch Points	Displays all the external touch points maintained. **Note:** 1) External touch points which are not part of any other group will be listed for selection. 2) Touch points which are already a part of any other group will be shown in disabled mode.

2. In the **Group Code** field, enter the unique group code for touch point group.
3. In the **Group Description** field, enter the touch point group description.
4. In the **Touch Points** field, select the checkbox against the Internal / External Touch Points.

Note: To select all available Internal / External Touch Points in one instance, select the checkbox adjacent to Internal / External Touch Points.

5. Click **Save** to save the Touch point group details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
7. The success message of Touch Point Group Maintenance saved successfully appears along with the transaction reference number.

FAQ

1. **From where can I get the list of touch points which I can club together?**

   Internal and external touch points maintained by the System Administrator using ‘Touch Point Maintenance’ will be listed for group creation.

2. **Can I club internal and external touch points together in one group?**

   No, clubbing of internal and external touch points together in one group is not allowed.

3. **Can I club one touch point as a part of multiple groups?**

   No, one touch point can be a part of only one group.

4. **Where can I use these touch point groups?**

   You can create a transaction limit package using ‘Limit Package Management’ for touch point group.

34. Role Maintenance

OBDX application has many roles for different type of users defined under different user types i.e. Retail & Business, Corporate, and Admin. These roles are defined for internal as well as for external touch points.

In case of Business user type, roles can be mapped at the time of specifying the Party Preference for Business type of party. The end user will be able to see/access only those transactions and widgets based on the roles mapped at the Party Level while inquiring about contextual information

Application roles mapped to Internal Touch Points (Internet, Mobile Application, SIRI, Chatbot, etc.) are used by OBDX itself, whereas Application roles mapped to External Touch Points are defined for being used by third party system. Each External role is mapped to a scope (defined in Identity Management System) and the same scopes are mapped to External Touch Points in **Touch Point Maintenance** screen.

For Internal Touch Points, a user can perform only those transactions which are mapped to the application role assigned to that user. Whereas for External Touch Points, third party system can only perform only those transactions (on behalf of the user), which are mapped to the application role, mapped to the scope assigned to that external touch point (third party system).

Using this option the system administrator can define an Application role alongwith entity information. However, mapping an Entity to a role is not mandatory. If no entity is mapped to an application role, it would be globally available across all entities. Factory shipped roles will be always ‘Global’ roles.

Application Roles are mapped to Entitlements for various Touch Points, so that System Administrator can decide which all transactions should be available for which touch points.

Apart from the transactions, OBDX widgets are also available as entitlement and can be mapped to the application roles.

System displays only those menu options widgets and dashboard which are mapped to the application role assigned to the logged in user. For e.g. If a user with application role ‘Retail’ does not have access to transactions widgets & dashboard related to Wealth Management module, then those transactions, widgets and dashboard will not be shown on the UI to user.

System Administrator user will be able to map transactions and privileges such as Perform, Approve and View, Release and Check to the various roles.

Note: The users can have access only to those transactions, dashboards and widget which are mapped to the role associated to the him/her.

Pre-Requisites

- Transaction access is provided to System Administrator.
- Approval rule set up for System Administrator to perform the actions.

Features supported in application

Using this option System Administrator can perform the following actions:

- Create Application Roles
- View Application Roles
- Edit Application Roles
- Delete Application Roles

How to reach here:

System Administrator Dashboard > Authorization and Access Controls > Role Maintenance
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Authorization and Access Controls > Role Maintenance

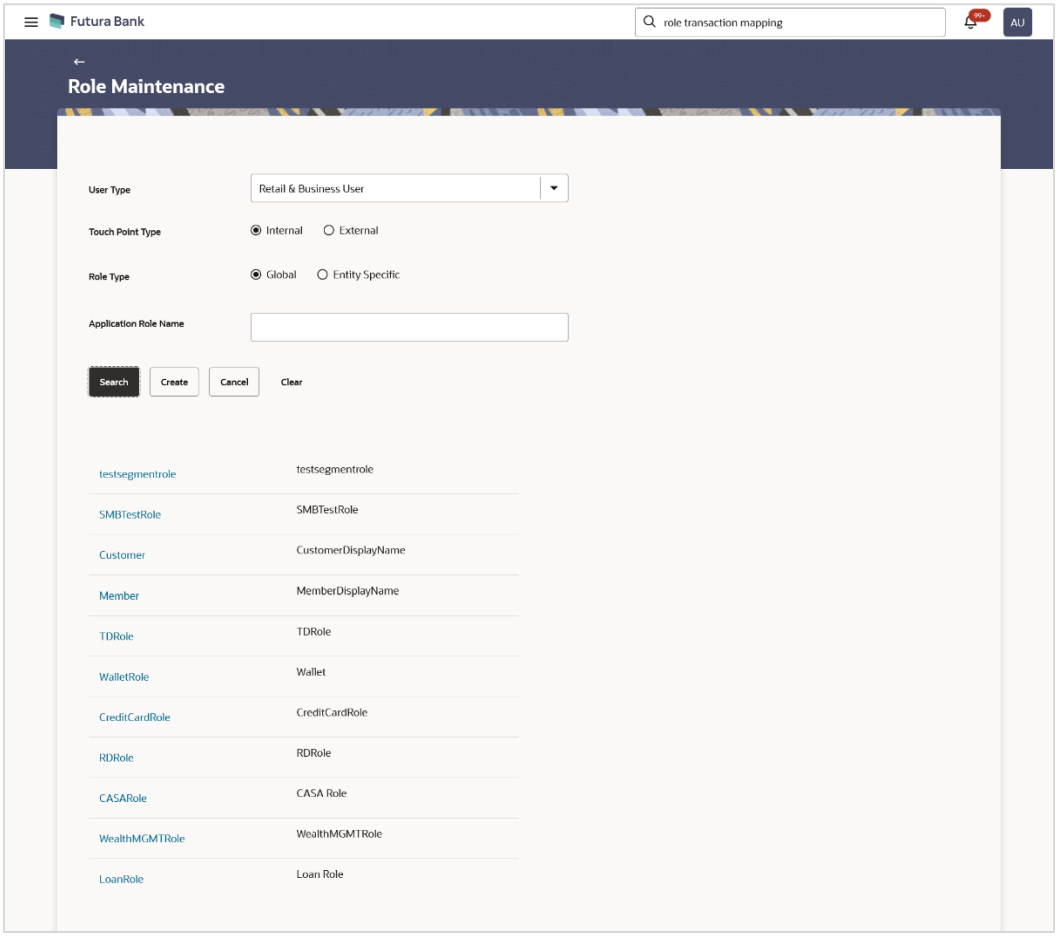
34.1 Search & View Application Role

Using this option, System Administrator can search application roles based on the search criteria. By default all the application roles will be displayed on this screen, Administrator can filter the list by entering the values in search criteria.

To search & view application role/ application roles:

1. In the **User Type** field, select the user type.
2. In the **Touchpoint Type** field, select desired option.
3. In the **Role Type** field, select the desired option. If entity specific is selected, the entity needs to be specified
4. In the **Application Role Name** field, enter the name of the application role.
5. Click **Search**.
   The search result based on search criteria displayed in **Application Role Details** section.
   OR
   Click **Clear** to reset the search parameters.
   OR
   Click **Cancel** to cancel the search process and to go back to dashboard.

Search Application Roles - Search Results



Field Description

Field Name	Description
User Type	User type for which the application role is created. Retail & Business User , Corporate User and Administrator are three user types available in the application.
Touchpoint Type	Type of the touchpoint. The options are: • Internal • External

Field Name	Description
Role Type	Type of the role. The options are: • Global • Entity Specific. For entity specific, the entity needs to be selected
Application Role Name	Name of the application role.

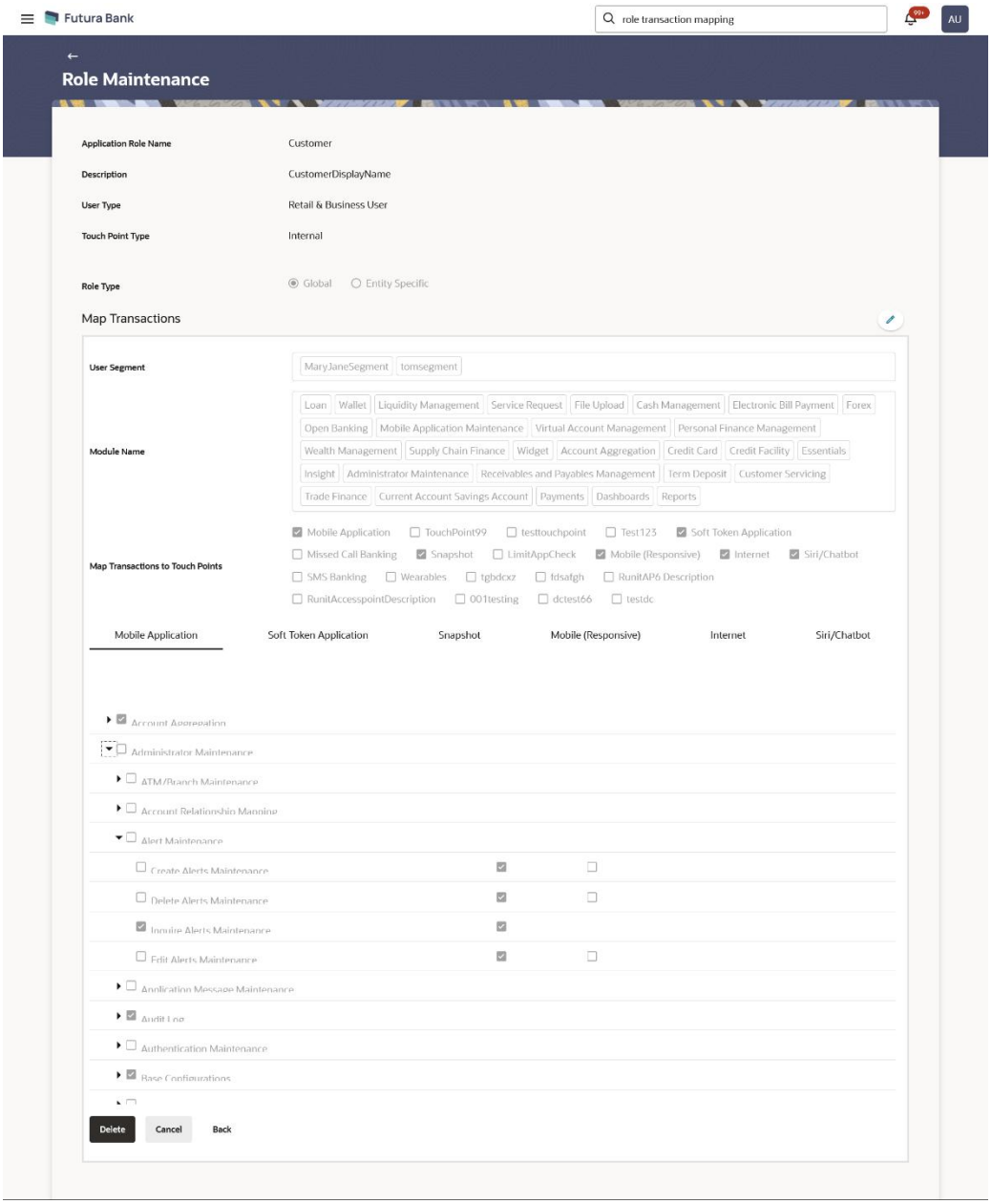
Application Role Details

Application roles can be views based on Touch Point Type-Internal and External in different tabs. Application roles are grouped and displayed User Segment wise.

Application Role Name	Name of the application role.
Application Role Description	Description of the application role.

6. Click on the **Application Role Name** to view the details. **Role Maintenance - View** screen appears.

Role Maintenance - View



Field Description

Field Name	Description
Application Role View	

Field Name	Description
Application Role Name	Name of the application role.
Description	Description of the application role.
User Type	User type for which the application role is created.
Touch Point Type	Type of Touch Point.
User Segment	Segment of the user for which the application role is created. This is applicable only for **Retail & Business user** type and **Internal** touch point type.
Map Transactions	
Module Name	Name of the module for which role transaction mapping is done.
Map Transactions to Touch Points	Touch points for which the transaction mapping is done for application role.
Transactions	Displays all the transactions for the selected module which are mapped to the application role for the selected touch points. Transactions are grouped under Transaction Categories and Module. The transactions are logically grouped for ease of mapping on **Role Transaction Mapping** screen.
Type of Action	Name of the action that can be performed for that transaction by the user to which this application role is assigned. • Perform- This action lets the user to perform or initiate those transactions and should be given to maker role. • View- This action lets the user to view the initiated and approved transactions by other users and should be given to viewer role. • Check- This action lets the user to check those transactions to which he/she has access and should be given to checker role. • Approve- This action lets the user to approve those transactions and should be given to approver role • Release- This action lets the user to release those transactions to which he/she has access and should be given to releaser role

7. Click against the particular category to view the transaction mapping details.

8. Click to modify the transaction role mapping. The **Role Maintenance** screen appears in editable form.
   OR
   Click **Delete** To delete the application role along with the transaction mapping. (Deletion of any role is only allowed if there are no users attached to that role)
   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click **Cancel** to cancel the search process and to go back to dashboard.

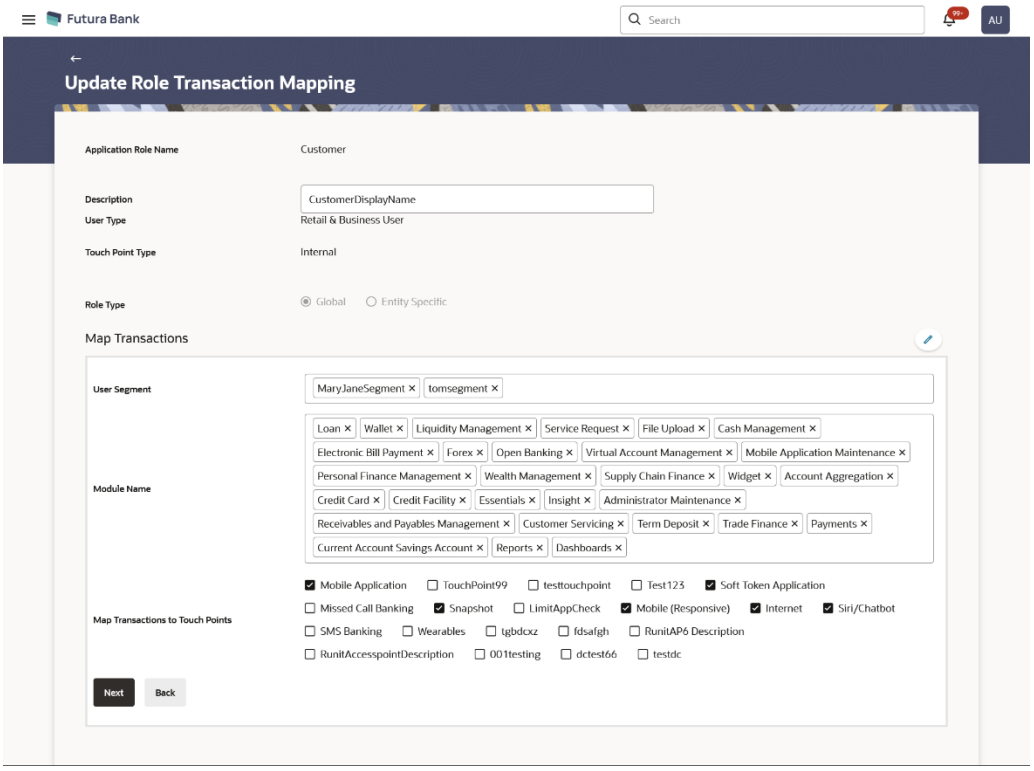
34.2 Edit Application Role

Using this option System Administrator can edit or update the details of an existing role transaction mapping.

To modify role transaction mapping:

1. Repeat step 1 to 4 of **Search Application Role** section.
2. Click against the **Map Transactions**.
   Screen in editable mode appears.

Role Maintenance - Edit

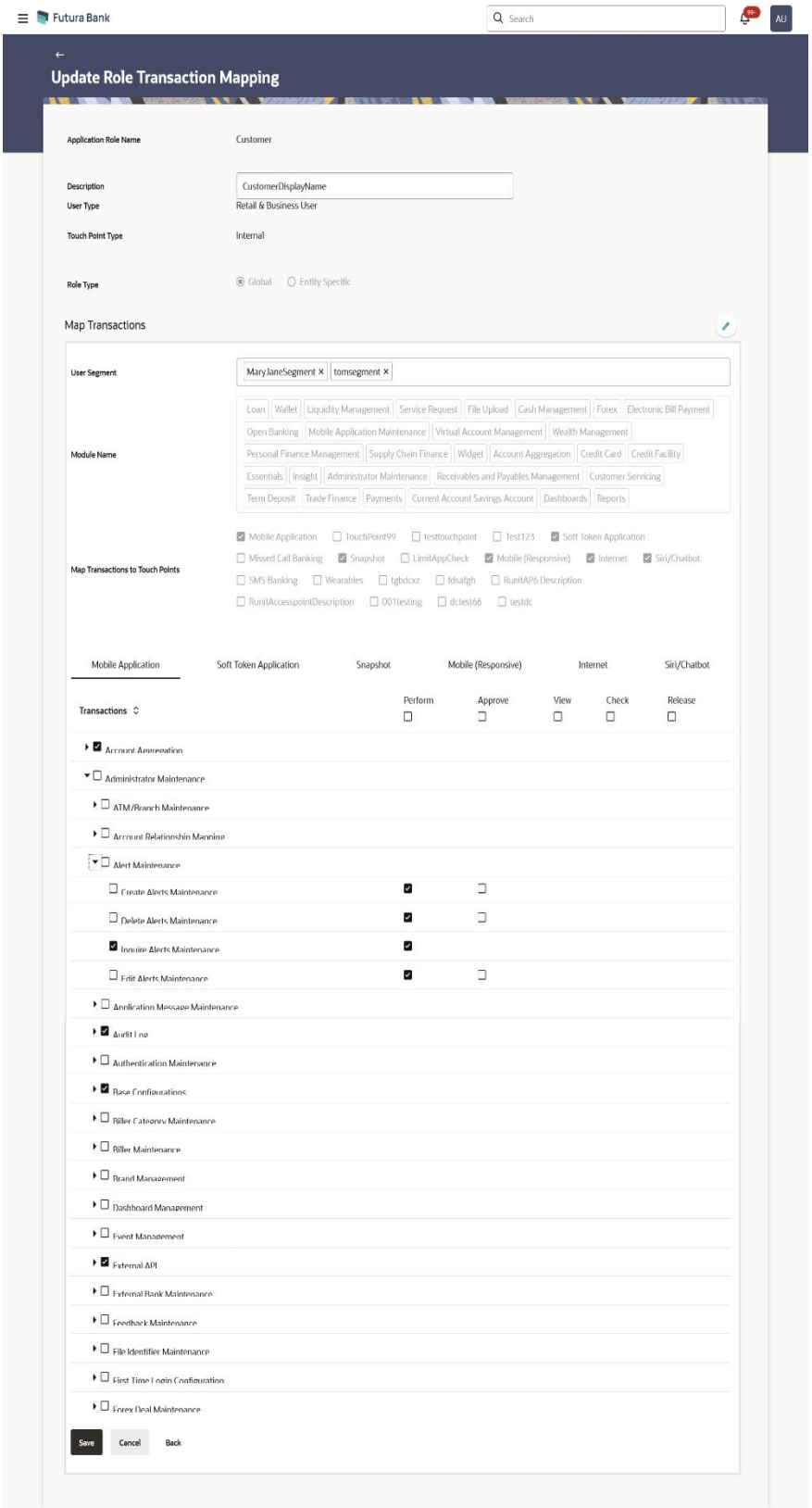


Note: Application Role Name, User Type, and Touch Point Type fields cannot be edited.

3. Update the role description if required.

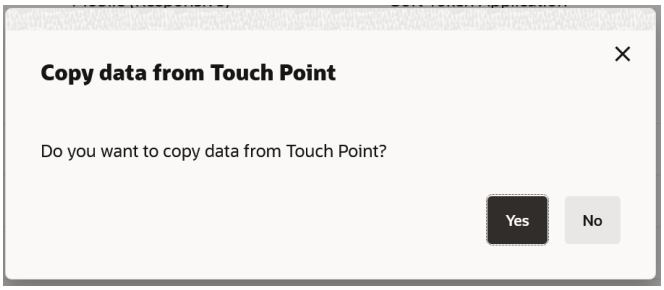
4. Add/ remove the user segment as per requirement.
5. Select/ deselect module names for which the transaction mapping is to be done.
6. Check/uncheck the touch points for which the transaction mapping is to be done.
7. Click **Next** to link/ delink transactions.
   OR
   Click **Back** to go back to previous screen.

Note: If the administrator deselects a module from Module name field, transaction mapping done for all the transactions under that module will get removed for that module. Similarly if the administrator unchecks and existing touch point, transaction mapping done for all modules for that touch point will get removed for that Touch Point.


Futura Bank
Search
AU
Update Role Transaction Mapping
Application Role Name
Customer
Description
CustomerDisplayName
User Type
Retail & Business User
Touch Point Type
Internal
Role Type
Global
Entity Specific
Map Transactions
User Segment
MaryJaneSegment
tomsegment
Module Name
Loan
Wallet
Liquidity Management
Service Request
File Upload
Cash Management
Forex
Electronic Bill Payment
Open Banking
Mobile Application Maintenance
Virtual Account Management
Wealth Management
Personal Finance Management
Supply Chain Finance
Widget
Account Aggregation
Credit Card
Credit Facility
Essentials
Insight
Administrator Maintenance
Receivables and Payables Management
Customer Servicing
Term Deposit
Trade Finance
Payments
Current Account Savings Account
Dashboards
Reports
Map Transactions to Touch Points
Mobile Application
TouchPoint99
testtouchpoint
Test123
Soft Token Application
Missed Call Banking
Snapshot
LimitAppCheck
Mobile (Responsive)
Internet
Siri/Chatbot
SMS Banking
Wearables
tghdcxz
fdsafgh
RunitAP6 Description
RunitAccesspointDescription
001testing
dctest66
testdc
Mobile Application
Soft Token Application
Snapshot
Mobile (Responsive)
Internet
Siri/Chatbot
Transactions
Perform
Approve
View
Check
Release
Account Aggregation
Administrator Maintenance
ATM/Branch Maintenance
Account Relationship Mapping
Alert Maintenance
Create Alerts Maintenance
Delete Alerts Maintenance
Inquire Alerts Maintenance
Edit Alerts Maintenance
Application Message Maintenance
Audit Log
Authentication Maintenance
Base Configurations
Biller Category Maintenance
Biller Maintenance
Brand Management
Dashboard Management
Event Management
External API
External Bank Maintenance
Feedback Maintenance
File Identifier Maintenance
First Time Login Configuration
Forex Deal Maintenance
Save
Cancel
Back

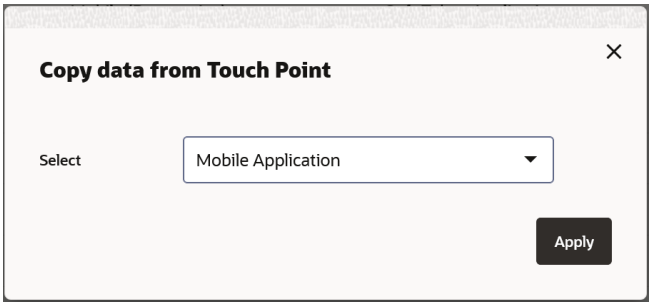
8. Modify the transactions mapping for different touch points. Click against the particular category to view and update the transaction mapping.
9. Click on the next touch point tab, a pop up window appears for asking **Copy data from touch point**.

Copy data from touch point Confirmation popup window



   a. Click **Yes** to select the touch point from which the data has to be copied.
   b. Copy transaction mapping details of touch point to another popup window.

Copy data from touch point Confirmation popup window



   a. From the **Select** list, select the touch point from the list.
   b. Click **Apply**.
      OR
      Click **No**. to do the mapping operationally.
10. Modify the transactions mapping for current touch points if required.
11. Click **Save** to save the updates.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate back to previous screen.
12. The screen with success message appears. Click **OK** to close the message screen.

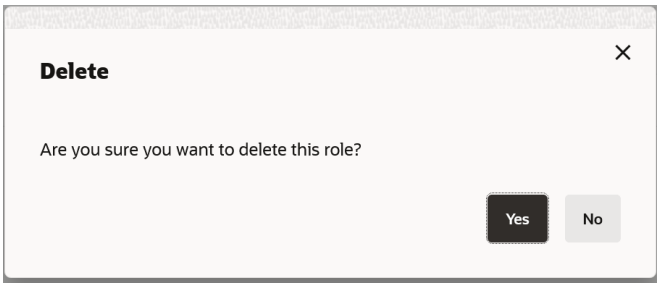
34.3 Delete Application Role

Using this option System Administrator can delete an existing role transaction mapping. Deletion of any role is only allowed if there are no users attached to that role.

To delete role transaction mapping:

1. Repeat step 1 to 4 of **Search Application Role** section.
2. Click **Delete** to delete the application role along with the transaction mapping.
   The **Delete Warning** message appears.

Delete Application Role



3. Click **Yes**.
   The **Role Maintenance** screen with the successful role deletion message appears.
   OR
   Click **No** to cancel the transaction.

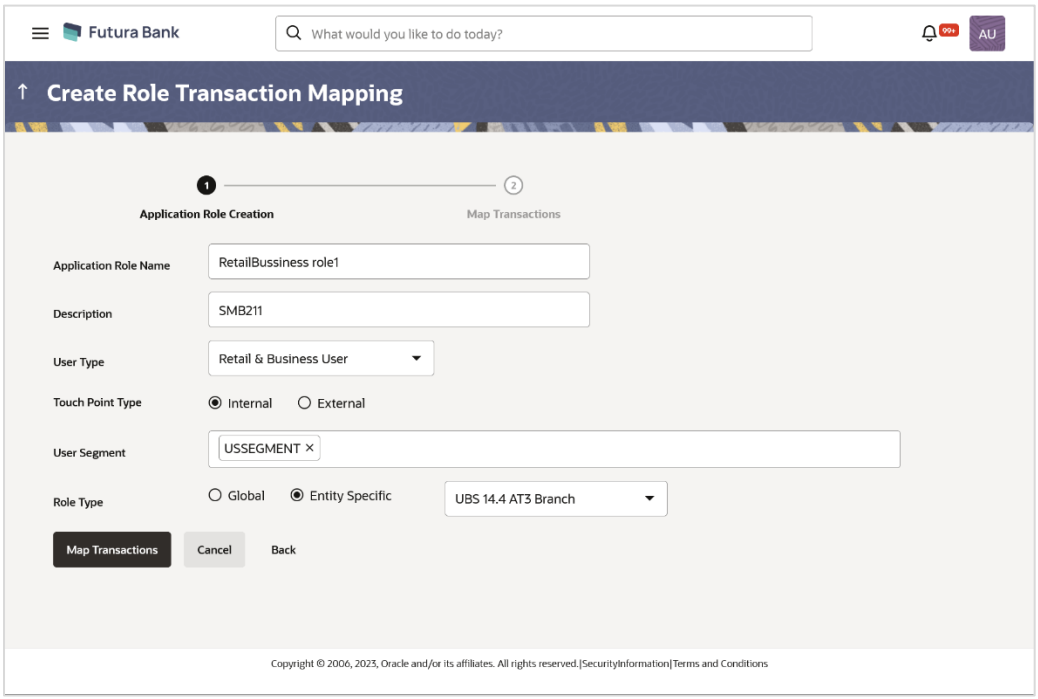
34.4 Create Application Role

Using this option System Administrator can define an application role and map transactions to it for selected touch points.

To create an application role transaction mapping:

1. In the **Role Maintenance** screen, click **Create**. The **Role Maintenance - Create** screen appears.

Application Role Creation



Field Description

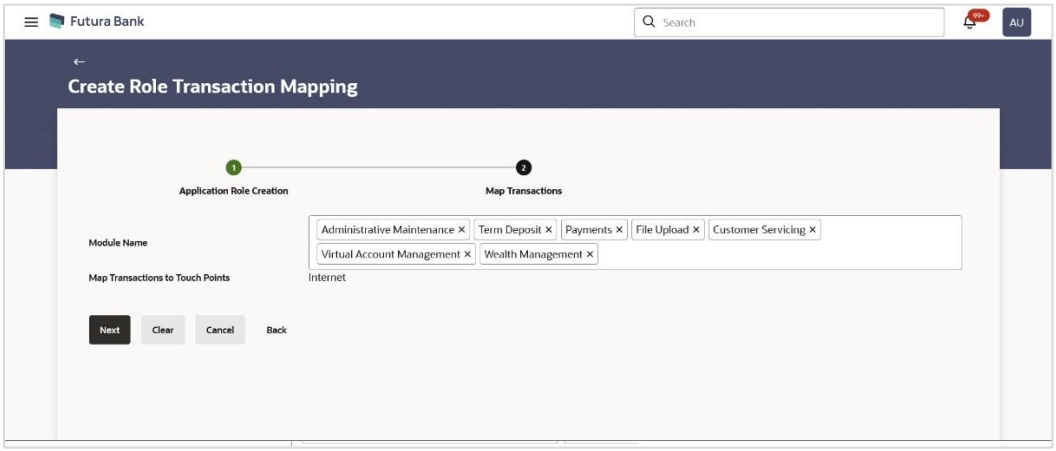
Field Name	Description
Application Role Name	Name of the application role.
Description	Description of the application role.

Field Name	Description
User Type	Type of the user for which the application role is to be created. The options are: • Retail & Business User • Corporate User • Administrator
Touch Point Type	Type of Touch Point. The options are: • Internal: (for internal touch points like internet, Mobile Application, Siri, Chatbot etc.) • External : (for third Party applications)
User Segment	User segments of selected user type for which the maintenance is to be done. This field is applicable only for **Retail & Business user type** and **Internal touch point** type.
Scope Name	List the scopes for the external touch point. This field is displayed and enabled, if you select **External** option in the **Touch Point Type** field. Once a scope is mapped to a role, it cannot be mapped to any other role.
Role Type	

2. In the **Application Role Name** field, enter the name of the application role.
3. In the **Description** field, enter the description of the application role.
4. From the **User Type** list, select appropriate type for which role is to be created.
5. From the **Touch Point Type** list, select appropriate option.
    a. If you select **External**;
        i. From the **Scope Name** list, select the appropriate scope to map to application role.
    b. If you select **Internal and User Type as Retail & Business**;
        i. From the **User Segment** list, select the appropriate segments for which maintenance is to be done.
        ii. If you select **Internal**;
            1. From the **Role Type** list, select the role type **Global** or If there is any specific role then select **Entity Specific**.
            iii. If you select **Entity Specific** option, then select the Entity specific role from list.

6. Click **Map Transaction** to map transaction to the role.
   The **Application Role Creation** screen to add transaction modules and touch points appears.
   OR
   Click **Back** to navigate back to previous screen.
   OR
   Click **Cancel** to cancel the transaction and to go back to dashboard

Role Maintenance - Application Role Creation



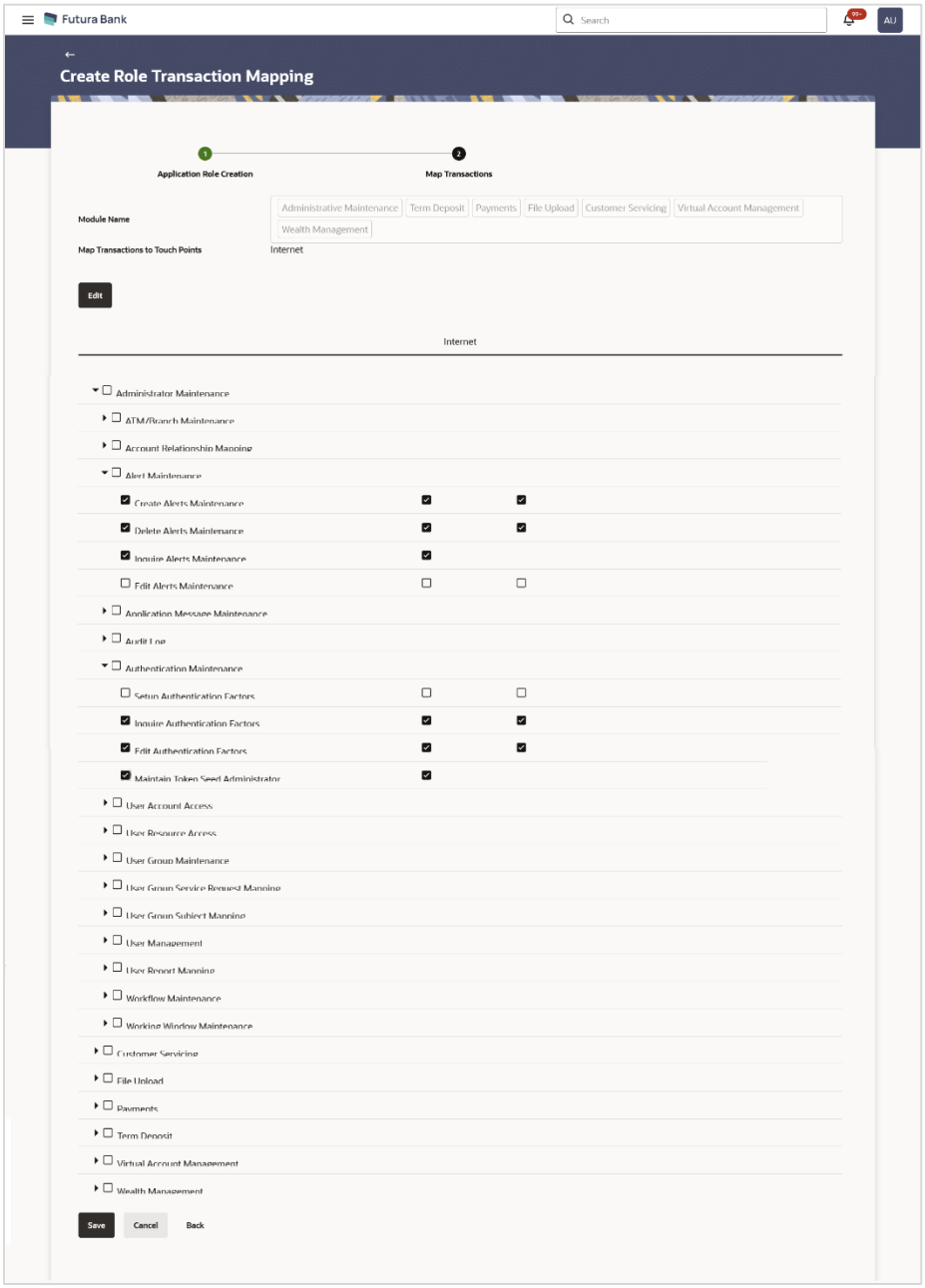
Field Description

Field Name	Description
Map Transactions	
In following section user can do entitlement mapping.	
Module Name	The modules for which the transaction mapping is to be done. Transactions under the selected modules will get displayed for mapping. Note: Select **All** option from the drop-down to select all modules.
Map Transactions to Touch Points	The internal touch points for which the transaction mapping is done for application role. All the internal touch point maintained in the system gets displayed here.

7. Select appropriate modules for transactions mapping.
8. Select the check box (against the list of Touch Points to map the transactions to selected touch points.

9. Click **Next**. The entitlement mapping section **Map Transaction** appears.
   OR
   Click **Clear** to reset the entered details.
   OR
   Click **Cancel** to cancel the transaction and to go back to dashboard.
   OR
   Click **Back** to navigate back to previous screen.

Role Maintenance - Map Transaction

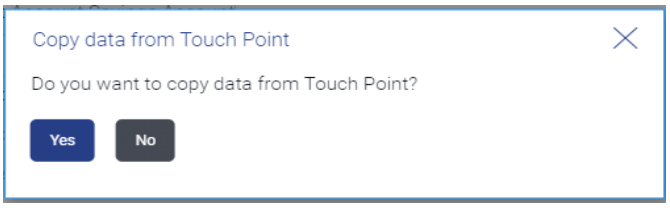


Field Description

Field Name	Description
Transactions	
Transaction Name	Name of transaction to be mapped to the application role. The transactions are logically grouped for ease of mapping on **Role Transaction Mapping** screen. Note: It is mandatory to map the transactions under the Essential category to the application role.
Action	Name of the action that can be performed for that transaction by the user to which this application role is assigned. • Perform- This action lets the user to perform or initiate those transactions and should be given to maker role. • View- This action lets the user to view the initiated and approved transactions by other users and should be given to viewer role. • Check- This action lets the user to check those transactions to which he/she has access and should be given to checker role. • Approve- This action lets the user to approve those transactions and should be given to approver role • Release- This action lets the user to release those transaction and should be given to releaser role

10. Click on the desired Touch Point tab for e.g. Internet.
11. To map the transactions to the role, click against the particular module, then select the transaction type, and then transactions to be mapped.
12. Select the respective check boxes preceding to transaction to be mapped.
    OR
    Select the checkbox at header level if you want to map all the transactions below that at one instance.
13. Click on the next touch point tab, a pop up window appears for asking **Copy data from touch point**.

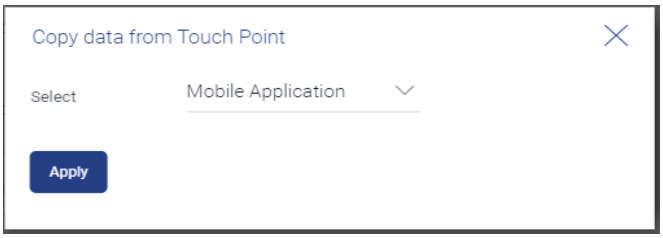
Copy data from touch point Confirmation popup window



a. Click **Yes** to select the touch point from which the data has to be copied.

b. Copy transaction mapping details of touch point to another popup window.

Copy data from touch point Confirmation popup window



a. From the **Select** list, select the touch point from the list.

b. Click **Apply**.
OR
Click **No**. to do the mapping operationally.

14. Click **Save** to save the changes.
OR
Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate back to the previous screen.

15. The **Role Maintenance - Review** screen appears. Verify the details, and click **Confirm**.
OR
Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate back to the previous screen.

16. The screen with success message of **Application Role Policy Map** appears. Click **OK** to complete the transaction.

FAQ

1. **Is it mandatory to map transactions to the created application role?**

   Yes. You will need to associate transactions for at least one module for a touch point, once an application role is created.

2. **Do I need to mandatorily map transactions for each touch point for the new application role created?**

   No, it is not mandatory to map transactions for each touch point for the new role created but if the same are not defined then on initiation of transaction from that touch point, system will give an access denied message.

3. **Why am I unable to select an action against a specific entitlement for a transaction?**

   This could be because that the specific action is not applicable or relevant for an entitlement i.e. approve as an action is not applicable to inquiry entitlement for a transaction.

4. **Can I copy the same transaction mapping for an application role from one touch point to another?**

   Yes, you can copy the details along with an option to decide from which touch point the details need to be copied. On selection of a touch point, system will prompt to select the touch point from which the entitlements need to be copied. If you had selected 'No' and later wish to copy the details, then you will need to click on the touch point tab again for the system to provide that option.

5. **Once I select the module and touch points for transaction mapping to an application, can I include additional modules and touch points?**

   Yes, you can click on 'Edit' and include additional modules and touch points for mapping.

6. **Can I associate multiple scopes to an application role of type external and how are they associated to external touch points?**

   No. Only one scope can be mapped to an application role to map transactions. Once a scope is mapped to an application role, that scope cannot be mapped to another application role. Multiple scopes can be associated to an external touch point as part of touch point definition and the same scope can be mapped to different external touch points.

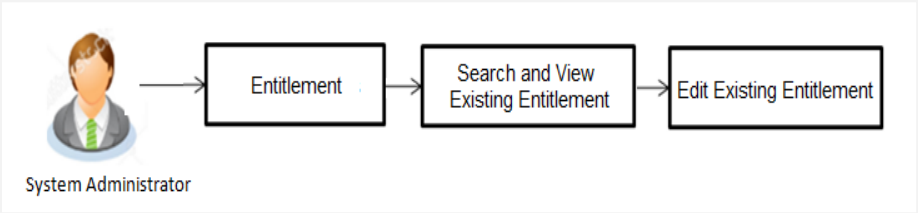
35. Entitlements

Entitlements are the transactions that the user can perform. Each Entitlement is linked to a single or group of resources. Access of these entitlements to a role is given basis on the necessity and relevance of entitlement to that role. For creation of role and mapping entitlements to that role please refer to Role Transaction Mapping screen.

Pre-Requisites

- Transaction access is provided to System Administrator.

Workflow



Features supported in application

Using this option system administrator can perform the following actions:

- View Entitlement
- Edit Entitlement

How to reach here:

System Administrator Dashboard > Authorization and Access Controls > Entitlements
OR
System/ Bank Administrator Dashboard >Toggle Menu > Menu > Authorization and Access Controls > Entitlements

35.1 Entitlements - View

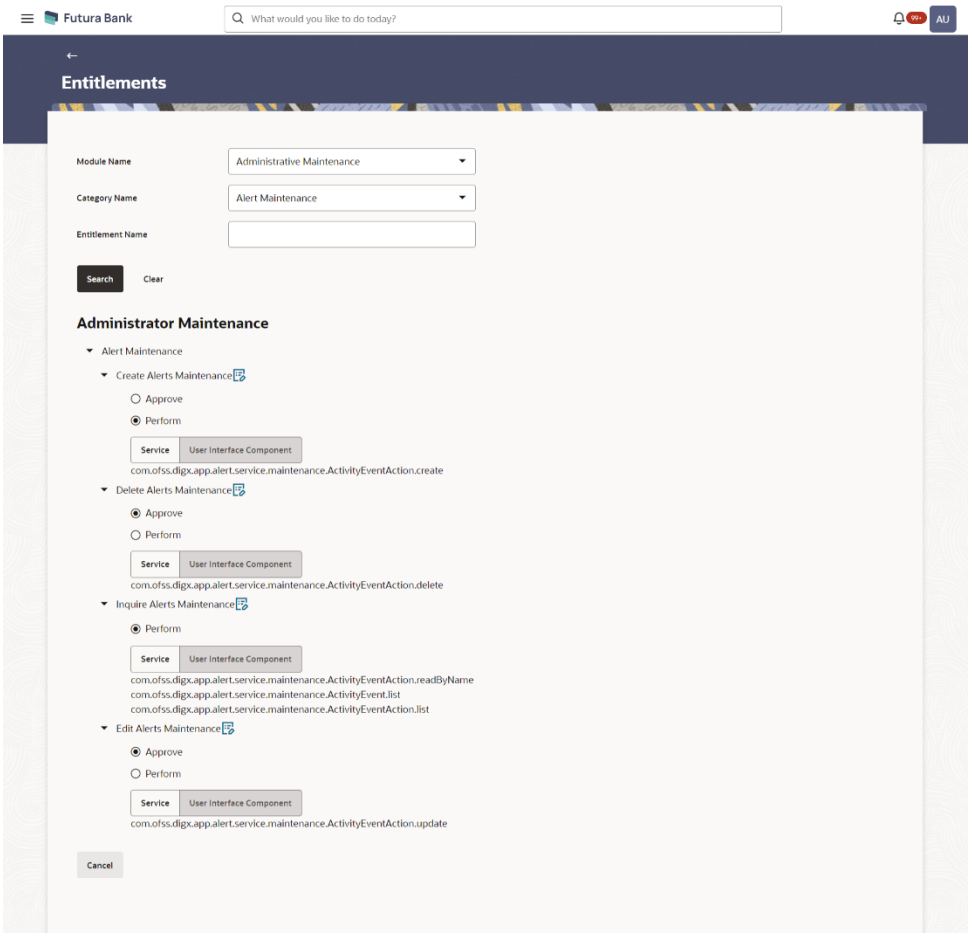
Using this option, Administrator can search and view the existing entitlements.

To search entitlement (s):

1. From the **Module Name** list, select the appropriate module for which the entitlements are to be viewed.
2. From the **Category Name** list, select the appropriate category of the selected module. 3. Enter the entitlement name.

3. Click **Search**. The based on the search criteria the list of entitlements appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the entered details.
   OR
   Enter the value directly in the **Entitlement Name** field and Click **Search**.

Entitlements - View



Field Description

Field Name	Description
Module Name	Name of the module under which all transactions are maintained. This field lists all the module names for the entitlements maintained in the system.
Category Name	Name of the category.

Field Name	Description
Entitlement Name	Name of entitlement/ transaction.
Entitlement Details	
Module Name	Name of the module under which all transactions/ entitlements are maintained.
Category Name	Name of the category under the module. Under each module entitlements are grouped under a category.
Transaction Name	Name of entitlement/ transaction.
Service	Displays the list of service resources mapped to the entitlements.
User Interface Component	Displays the list of user interface components mapped to entitlements.
Action Name	Name of available actions for an entitlement. The options are: • Approve • Perform • View
Resource Name	Name of the resources mapped to entitlement for each action-Approve/Perform/View under Services or User Interface Component.

4. Click against the particular category to view the entitlement under that category.
5. Select the **Service** or **User Interface Component** tab to view respective details.
6. Click to update entitlement details.
   OR
   Click **Cancel** to cancel the transaction and go back to dashboard.

35.2 Entitlements - Edit

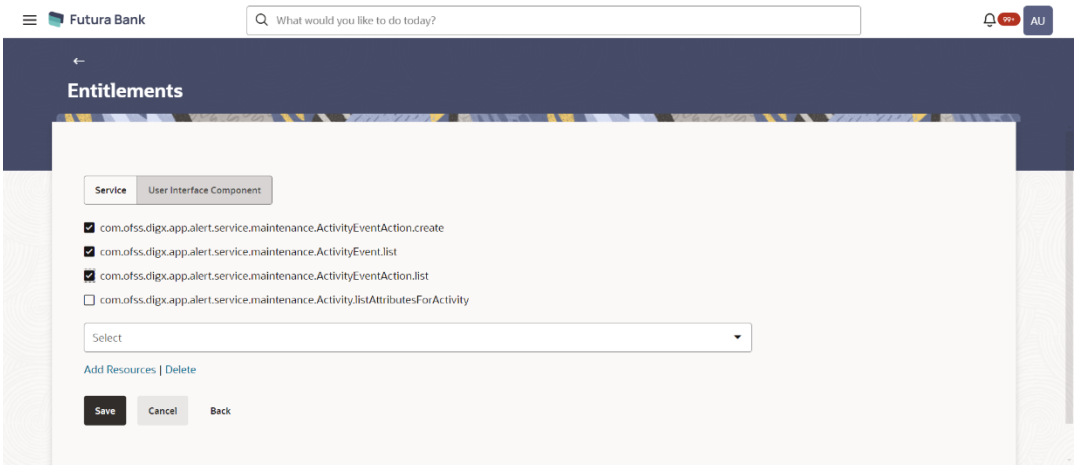
Using this option, Administrator can add or delete the resources under Services and User Interface Component.

To update entitlement details:

1. From the **Module Name** list, select the appropriate module for which the entitlements are to be viewed.

2. From the **Category Name** list, select the appropriate category of the selected module. 3. Enter the entitlement name.
3. Click **Search**. The based on the search criteria the list of entitlements appears.
   OR
   Enter the value directly in the **Entitlement Name** field and Click **Search**.
4. Click against the particular category to view the entitlement under that category.
5. Click to update entitlement details. The **Entitlements - Edit** screen appears.

Entitlements - Edit



Field Description

Field Name	Description
Module Name	Name of the module under which all transactions are maintained. This field lists all the module names for the entitlements maintained in the system.
Category Name	Name of the category.
Entitlement Name	Name of entitlement/ transaction.
Service	Displays the list of service resources mapped to the entitlements.
User Interface Component	Displays the list of user interface components mapped to entitlements.

Field Name	Description
Action Name	Name of available actions for an entitlement. The options are: • Approve • Perform • View
Resource Name	Name of the resources mapped to entitlement for each action-Approve/Perform/View under Services or User Interface Component.

6. Select the **Service** or **User Interface Component** tab to update the respective details.
7. Click **Add Resources** link to add resource. This field populates all the existing resources in the system for selection.
   OR
   Select the existing resources and click **Delete** link to delete the selected resource.
8. Click **Save** to save the changes made to the entitlements.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
9. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
10. The success message of entitlements updation appears.
    Click **OK** to complete the transaction.

36. User Segment Maintenance

In order to offer appropriate product and services to the customers, banks can employ some method of segmentation. Banks can group customers into different segments on the basis of different attributes of the customer; it could be demographic information, geographical information, behavioral information etc.

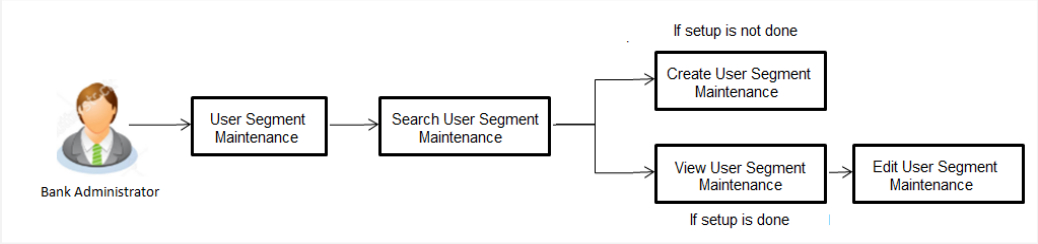
Banks can have different communication mailers, authentication mechanisms, transaction limits and branding aspects on the basis of customer segmentation.

User segment maintenance screen allows the system administrator to create new segments and subsequently use these segments to define specific maintenances at user segment level. Limits can also be defined specific to a user segment. Within each user segment, limits package can be associated to different touch points.

Pre-Requisites

- Transaction access is provided to System / Bank Administrator.
- Application roles are maintained

Workflow



Features Supported In Application:

- Create User Segment
- Search and View User Segment
- Edit User Segment

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Authorization and Access Controls > User Segments Definition
OR
System/ Bank Administrator Dashboard > Authorization and Access Controls > User Segments Maintenance

36.1 User Segment Maintenance - Search

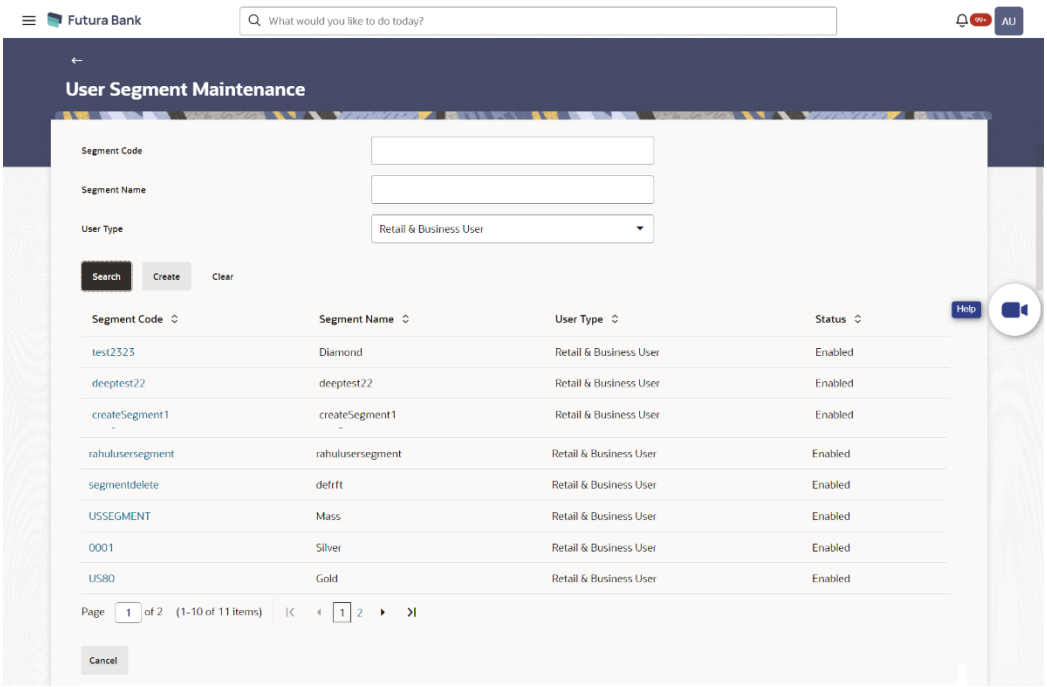
Using this option, System Administrator user can search the user segments maintained for retail users. The search result displays matching results based on search criteria entered.

System Administrator can view details of a specific segment by selecting the segment ID to get required details for a segment.

To search user segments:

1. In the **Segment Code** field, enter the segment code whose details you want to view.
   OR
   In the **Segment Name** field, enter the name of the segment whose details you want to view.
   OR
   From the **User Type** list, select the user type for which you wish to view user segment details. Currently only segments for user type 'Retail' can be defined.
2. Click **Search**.
   The search results appear on the **User Segment Maintenance** screen based on the search parameters.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction and the administrator will be navigated back to the **Dashboard**.

User Segment Maintenance- Search Result

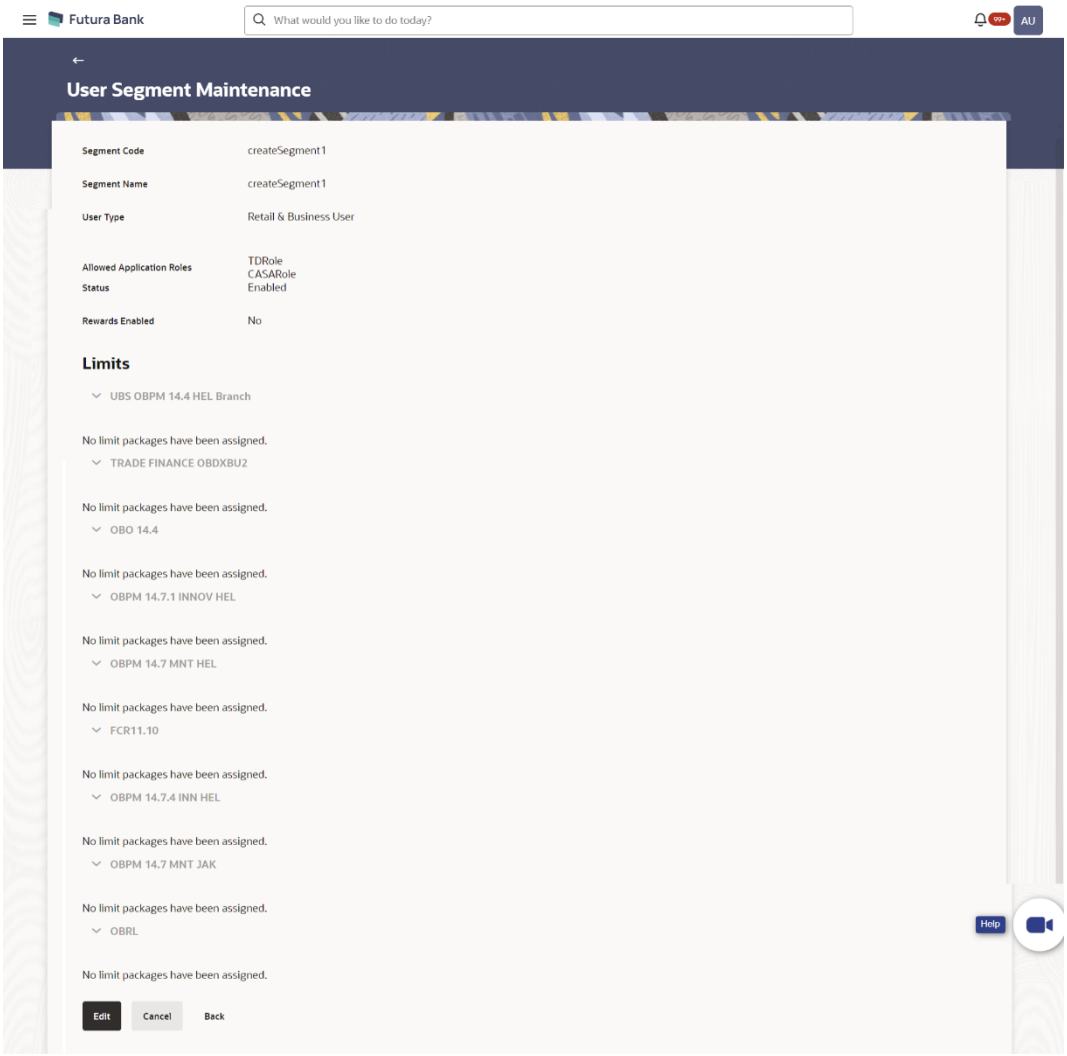


Field Description

Field Name	Description
Search Parameters	
Segment Code	Enter the segment code of the segment that needs to be searched.
Segment Name	Enter the name of the segment that needs to be searched
User Type	Select the user type for which segment details needs to be searched
Search Result	
Segment Code	System displays the code of the segment(s) based on the search criteria input.
Segment Name	System displays the name of segment(s) based on the search criteria input.
User Type	System will display the user type i.e. Retail / Corporate against each of the search result.
Status	System displays the status of the segment whether it is active/inactive.

3. Click the **Segment Code** link of the record for which you want to view the user segment details. The **User Segment Maintenance - View** screen appears.

User Segment Maintenance- View



Field Description

Field Name	Description
Segment Code	System displays the Segment Code of the segment that was selected to view details.
Segment Name	System displays the name of the segment that was selected to view details.
User Type	System displays the user type of the segment that was selected to view the details.
Allowed Application Roles	System displays the application roles that are mapped to the selected segment.
Status	System displays the current status of the selected segment i.e. whether the segment is active / inactive. Note: If the user segment is no longer active and needs to be disabled then the same can be done in **Edit** mode.

Limits - Touch Points /Group/ Global

Limits package can be optionally attached at user segment level. All the touch points and touch point groups maintained in the system are listed under each entity in case of multi entity setup. Limits Package can be mapped for each touch point and for a touch point group.

Touch Points/ Group/ Global	Name of touch points/ groups/ global under a specific entity (with all internal and external touch points).
Internal Touch Points Group for All	Displays the touch points which are the part of a group.

Field Name	Description
Touch Points	Displays the touch points (banking channels) which allows a user to perform transactions using the touch points. The touch points could be: • Mobile Application • Mobile (Responsive) • Internet • Mobile Banking • Missed Call Banking • SMS Banking • Wearables • Snapshot • Siri / Chatbot

4. Click **Edit** to modify the segment details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.

36.2 User Segment Maintenance - Edit

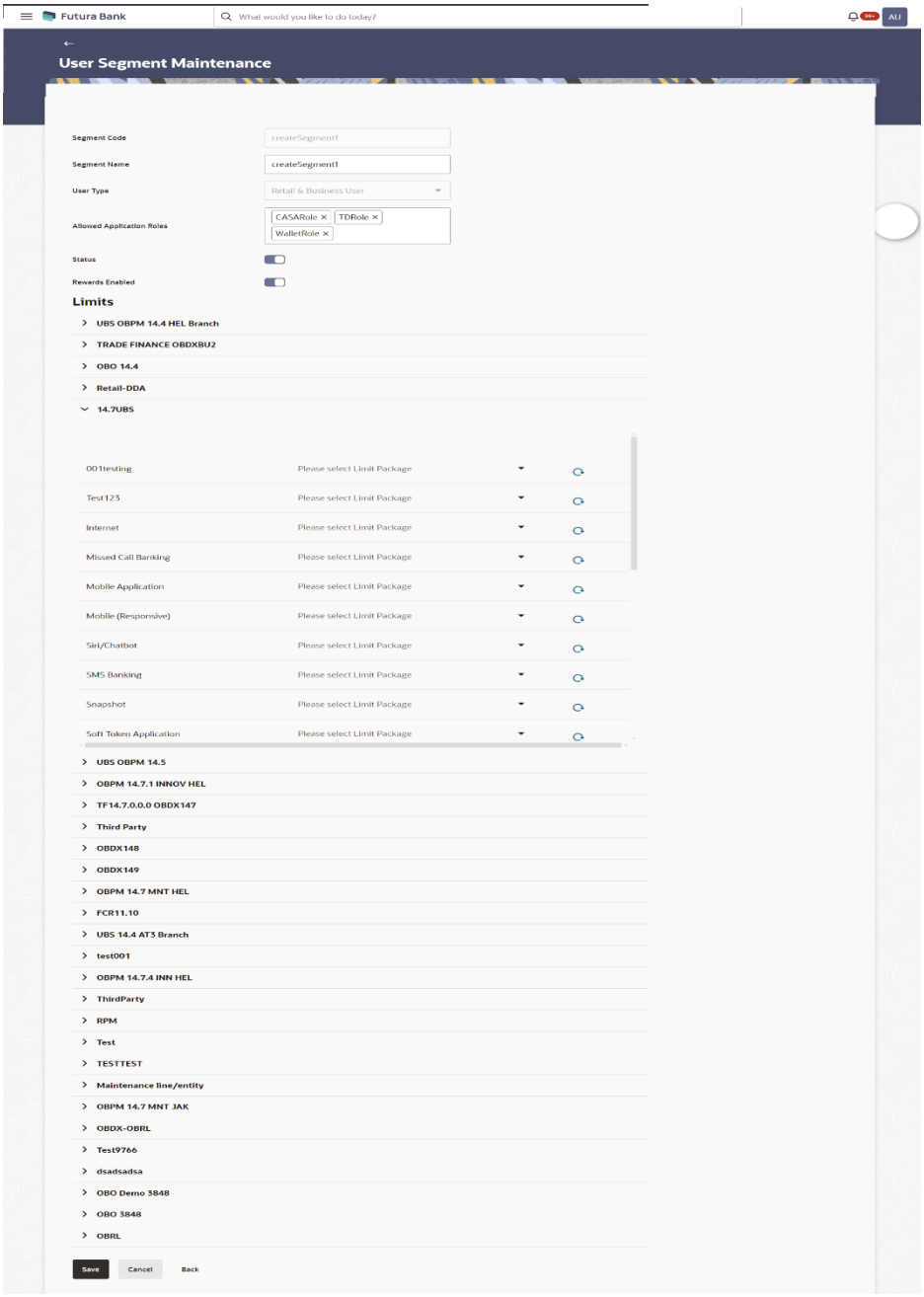
Using this option, System Administrator can modify the details of the existing user segment.

To edit the user segment details:

1. In the **Segment Code** field, enter the segment code whose details you want to modify.
   OR
   In the **Segment Name** field, enter the name of the segment whose details you want to modify.
   OR
   From the **User Type** list, select the user type whose user segment details you want to modify.
2. Click **Search**.
   The search results appear on the **User Segment Maintenance** screen based on the search parameters.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction. The **Dashboard** appears.
3. Click the **Segment Code** link of the record to select the segment for which you want to modify the details. The **User Segment Maintenance - View** screen appears.

4. Click **Edit** to modify the User Segment details.
   The **User Segment Maintenance - Edit** screen appears. .

User Segment Maintenance- Edit



Field Description

Field Name	Description
Segment Code	System displays the segment code of the segment selected and is non-editable.
Segment Name	System displays the name of the selected segment and is available for edit.
User Type	System displays the User type for the selected segment and is non-editable
Allowed Application Roles	System displays the application roles that have been mapped to the selected segment and are available for edit. As part of edit, new application roles can be mapped and existing roles can be removed.
Status	System displays the current status of the user segment and is available for edit. **Note**: You can modify the segment status to Active if the current state is Inactive and vice-versa.

Limits

Limit - Touch Points /Group

Limits package can be optionally attached at user segment level. All the touch points and touch point groups maintained in the system are listed under each entity in case of multi entity setup. Limits Package can be mapped for each touch point and for a touch point group.

Touch Points/ Group	Name of touch points/ groups maintained under a specific entity to which the limit packages can be mapped.
Package	System lists the packages available for mapping to a touch point/ touch point group. If there was any limits package to a touch point/group mapped earlier, it will be shown in editable form.
Actions	Click to reset the limit packages defined for a segment.

5. Edit the required details i.e. segment name, allowed Application Roles, Status, and Limits package for any of the touch point/touch point group.
6. Click **Save** to update the changes.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.

7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to make changes if any.
   OR
   Click **Cancel** to cancel the transaction and navigate back to **Dashboard**.
8. The success message of modification appears.
   Click **OK** to complete the transaction.

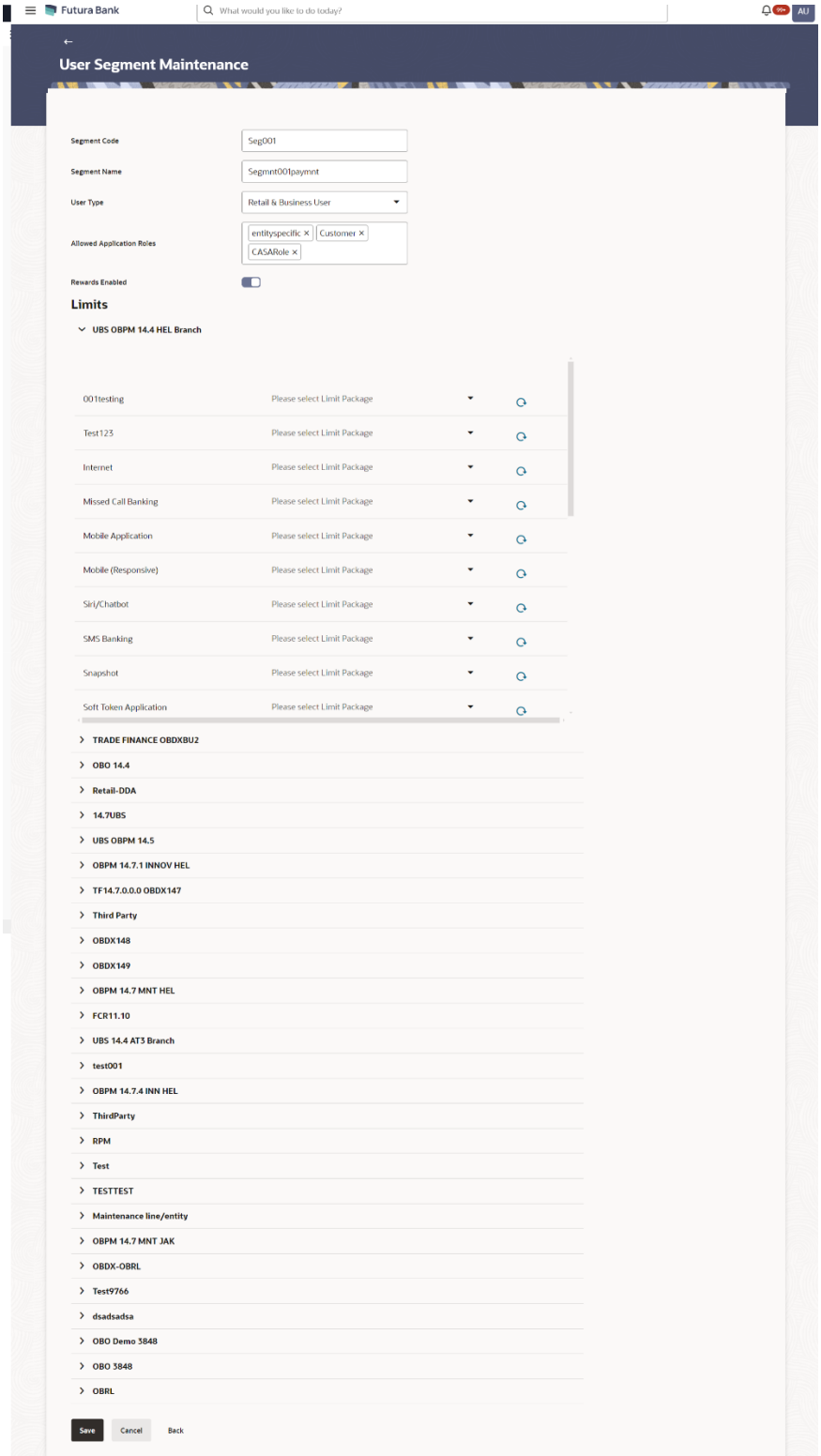
36.3 User Segment Maintenance - Create

Using this option, System Administrator can create new user segment for a user type ‘Retail’.

To create the user segment:

1. In the **User Segment Maintenance** screen, click **Create**. The **User Segment Maintenance - Create** screen appears.

User Segment Maintenance- Create



Field Description

Field Name	Description
Segment Code	Enter the unique code for the user segment to be created.
Segment Name	Enter the name of the user segment to be created.
User Type	Select the User type from the list for which the user segment is to be created. Currently only user type 'Retail' is supported
Allowed Application Roles	Select the application role(s) that needs to be associated to the user segment being created. The selected application role(s) will be by default available to the users to whom the created segment is associated.
Limits	
Limit - Touch Points /Group	
In this section user can define limits package for a user segment so that, bank can have varying limits depending on the segment of the user.	
Touch Points/ Group	Name of touch points/ groups maintained under a specific entity to which the limit packages can be mapped. **Note**: The limits package will be associated to a touch point/touch point within a segment. It is not mandatory to associate limits package to each touch point / touch point group.
Package	Select the limits package from the list of packages available for mapping to a touch points/ groups.
Actions	Click to reset the limit packages selected against the touch point.

2. In the **Segment Code** field, enter the unique code for the user segment to be created.
3. In the **Segment Name** field, enter the name of the user segment to be created.
4. In the **User Type** list, select the appropriate user type for the user segment being created.
5. In the **Allowed Application Roles** list, select the application role(s) to be mapped to the segment.
6. In the **Limits** section, select the limit packages to be mapped to touch points / touch point from the limit package list. The limits package selected as part of this definition will be applicable to the users to whom this segment is associated and will also depend on the limits preference applicability.

Note: Click to reset the limit packages applicable to a segment.

7. Click **Save** to save the user segment details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
8. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
   The user will be navigated back to the create screen.
9. The success message of transaction completion appears.
   Click **OK** to complete the transaction.

FAQ

1. Is it mandatory to create a User Segment as part of Day 1 maintenances?

No. It is not mandatory to create User Segments as part of Day 1 definition. If User Segments are created, then the same will be available for association to user as part of User Onboarding but it is not mandatory to associate user segment to business users as part of onboarding.

2. What is the relationship between User Segment and Application Roles?

Association of application roles to user segment is not mandatory. Multiple application roles can be assigned to a user segment and those application roles will be by default available to all users who are assigned that segment. The same application role can be mapped to multiple user segments.

3. **Can I remove specific application role(s) from the user level if I associate user segment?**

The application role(s) that are mapped to a user segment cannot be removed from the user if the segment is associated to the user, however the application role(s) that are not associated to any user segment will be available for mapping/unmapping at user level.

4. What will happen if I disable a Segment which is associated to Users?

Access to all the maintenances done on that segment level like Dashboard Builder, Product mapping, 2FA, Limits will not be referred. System will start referring to the maintenance done for the User Type associated to the users attached to the disabled segment, for Dashboard Builder, Product mapping, 2FA and Limits.

Users associated to the disabled segment will not have access to the application roles attached to that segment, hence bank user should attach new segment or application operationally to those users.

37. Authentication

Passwords are the most common form of authentication used in the world today. But passwords can easily be forgotten and commonly compromised. Two-factor authentication (2FA) adds an extra layer of security by requiring users to use two different authentication factors to verify their identity.

The two step verification or 2 Factor Authentication is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only, and only, the user knows e.g. tokens, OTP, answer of security questions etc. Using a Two Factor Authentication process can help to lower the number of cases of identity theft on the Internet, as well as phishing via email. For security reason authentication is used by user (Retail/ Corporate) while performing transactions through digital platform.

The Two Factor Authentication requires two different kinds of evidence before executing transaction successfully. This option enables the System Administrator to maintain authentication pattern for each transaction of a specific user segment.

Second Factor authentication can be set for each User type (Retail & Corporate) and for user type and User Segment combination (as of now user segment is only available for Retail user type).

This maintenance can be setup for each entity in a multi entity setup, which enables banks in defining different authentication mode for a same transaction for each entity.

In a multi entity setup, if the user is changing his entity, post login, then system should ask for second factor authentication.

The types of 2 factor authentication used are as follows:

- OTP : A onetime password will sent on user's registered mobile number or email id .
- Security Questions: User will be asked to answer the security questions set up by him.
- Random Number based Soft Token: The token randomly changes on the soft token app after the system defined time, and user will be required to enter the same on screen to authenticate the transaction.
- Time based Soft Token : It is a time based soft token that gets generated on the soft token application. Token gets expired after a defined time and user will be required to generate a new token.
- Push Notifications based 2FA :User will get a push notification to authenticate and complete a transactions on his registered device (mobile/wearable), on initiation of a transaction from a different form factor .
- Since the user is required to authenticate the transaction on the device where he has received the push notification, It acts as an additional security wherein the user can approve/reject the transaction only from his registered device. For receiving push notifications user should allow the same for the respective app on his device.

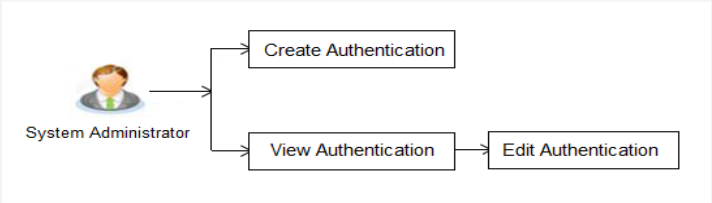
Note: Two factor authentication is only for retail and corporate user.

Pre-requisites

- Transaction access is provided to System Administrator.

- Approval rule set up for Bank Administrator to perform the actions.
- Transactions are enabled for 2 Factor Authentication aspect.

Workflow



Features Supported In Application

The following options are available as part of this maintenance:

- View Authentication
- Edit Authentication
- Create Authentication

How to reach here:

System/ Bank Administrator Dashboard > Security > Authentication
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Security > Authentication

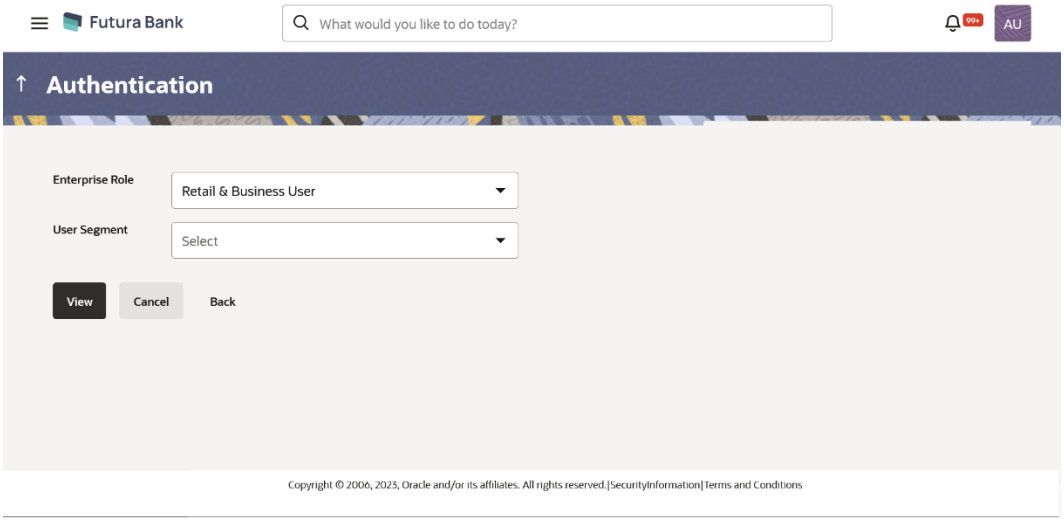
37.1 Authentication - View

On accessing 'Authentication' menu, system displays the existing maintenance available for selected user segment to view the authentication setup for user segment:

To view the authentication setup for user segment:

1. From the **Enterprise Role** list, select the appropriate role.
2. From the **User Segment** list, select the appropriate user segment.

Authentication Setup



Field Description

Field Name	Description
Enterprise Role	Name of enterprise roles set in application. The options are: • Retail User • Corporate User
User Segment	The user segments maintained by the Bank (applicable for Retail User type only).

3. Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to go back to Dashboard.
   OR
   Click **View** to view the 2FA maintained for the user segment. The **Authentication - View** screen appears.

Note:
1) If the existing maintenance is not available for selected user segment, message will be displayed "2 Factor Authentication for this user segment has not been set up yet" with the **Set up now** button which launches the screen to maintain 2 Factor Authentication.

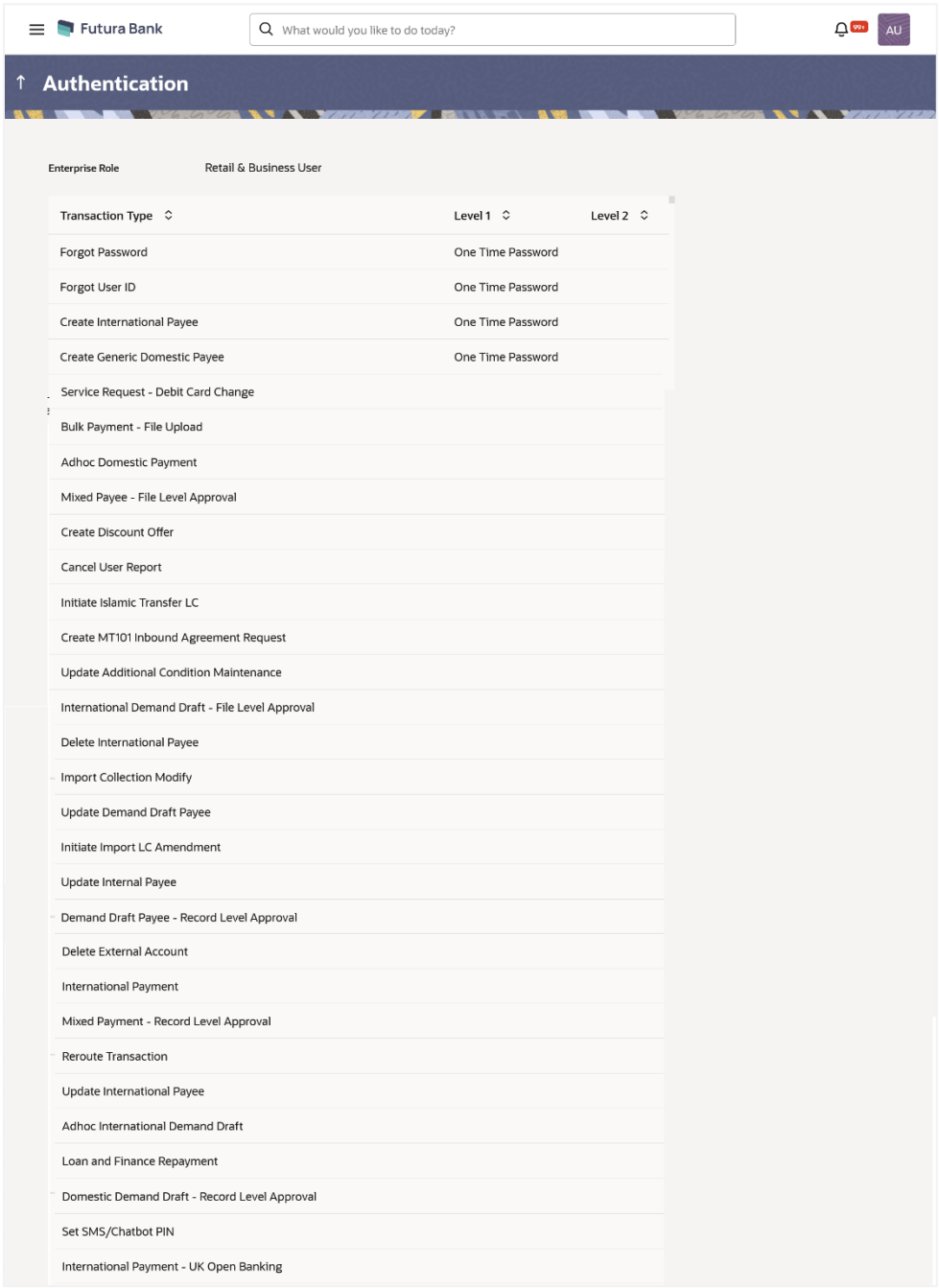
2) Only OTP should be maintained as the second factor authentication mode for ‘Wallet Registration’ event. Other second factor authentication modes like Soft Token and Security Questions are not supported for this event.
3) 2FA mode Push Notification based 2FA is not supported for the following transactions:

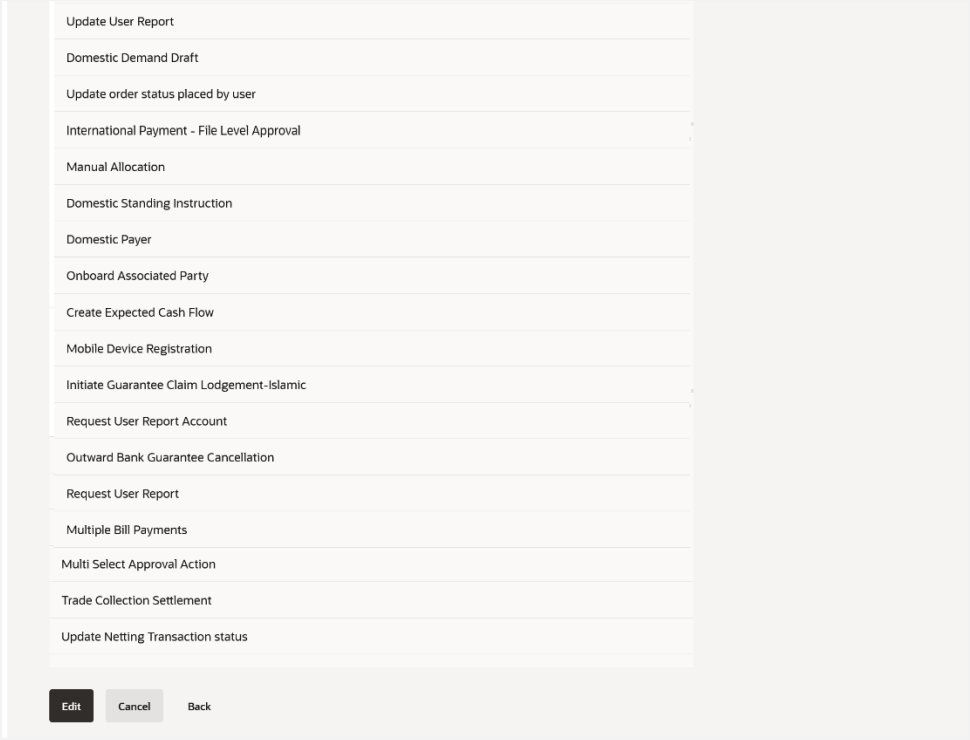
- Login
- Push Notification registration
- Soft Token registration

4) If the user is changing his entity post login, system will check the 2FA mode configured for Login event for the changed/destination entity, and if the 2FA mode for ‘Login’ event is different for the changed/destination entity then the user will be asked for the incremental second factor authentication (as per the setup).
5) If the 2FA mode is same for both the entities, then on switching the entity user will not be asked for any second factor authentication.
6) Following modes of 2FA will be supported on Login event :

- OTP
- Soft Token

Authentication Setup- View





Field Description

Field Name	Description
View	
Enterprise Role	View the enterprise role for which the 2 Factor Authentication is set-up.
User Segment	View the user segment for which the 2 Factor Authentication is set-up.
Transactions	
Transaction Type	The transaction type for which the 2 Factor Authentication is set-up.
Level 1	Displays the first level of two factor authentication mode (Security Questions, One Time Password, Soft Token, Push Notification based 2FA) set for the transaction type.
Number of Question	Number of security questions to be asked from user at level 1 authentication. This field appears only if the **Security Question** option is selected as the **Authentication mode**.

Field Name	Description
Level 2	Displays the second level of two factor authentication mode (Security Questions, One Time Password , Soft Token, Push Notification based 2FA) set for the transaction type.
Number of Question	Number of security questions to be asked from user at level 2 authentication. This field appears only if the **Security Question** option is selected in the **Authentication**.

4. Click **Edit** to update the details. Screen in editable mode appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to go back to previous screen.

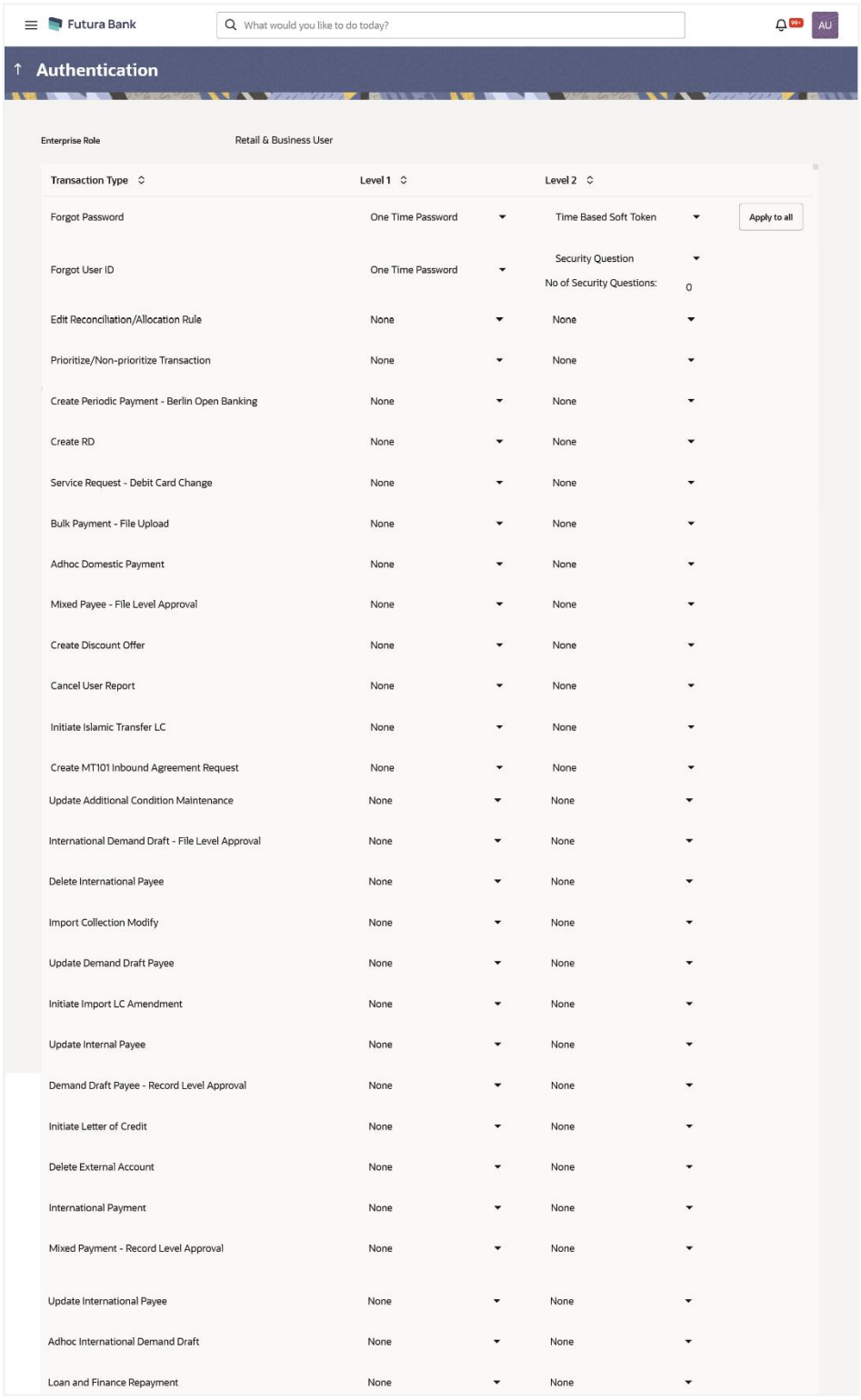
37.2 Authentication - Edit

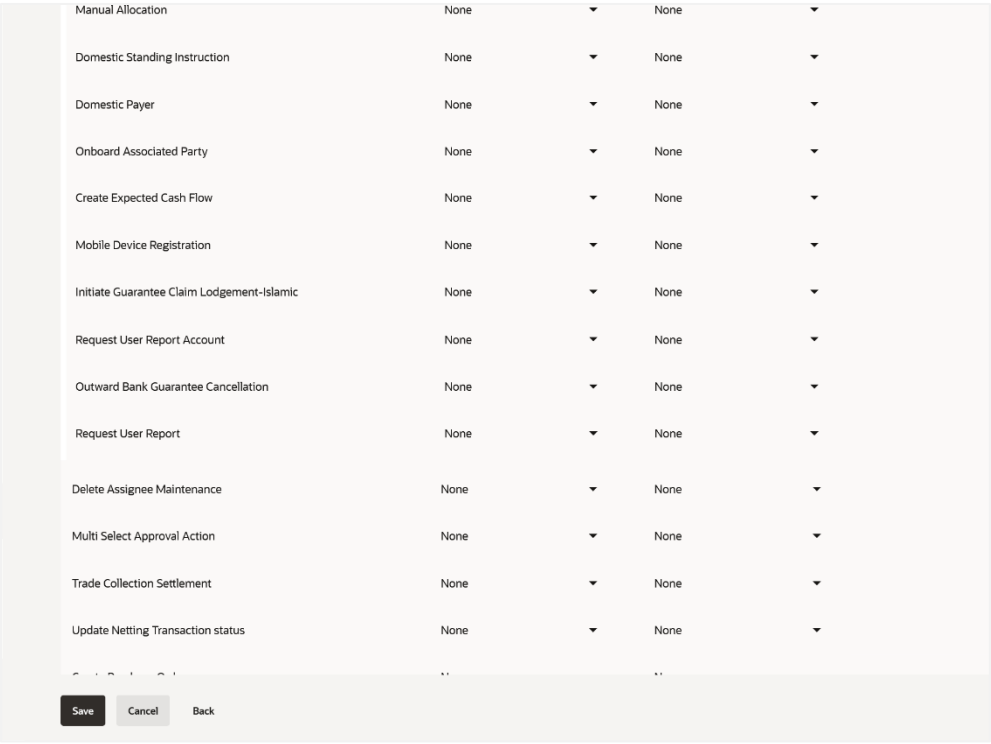
System Administrator can modify existing authentication maintenance.

To edit the authentication setup:

1. From the **Enterprise Role** list, select the appropriate role.
2. From the **User Segment** list, select the appropriate user segment (if applicable).
3. Click **View** to view the 2 Factor Authentications maintained for the user segment. The **Authentication - View** screen appears.
4. Click **Edit**. The **Authentication – Edit** screen with values in editable form appears.

Authentication - Edit





Field Description

Field Name	Description
Edit	
Enterprise Role	The enterprise role for which the 2 Factor Authentication is set-up.
User Segment	The user segment for which the 2 Factor Authentication is set-up.
Transactions	
Transaction Type	The transaction type for which the 2 Factor Authentication is set-up.

Field Name	Description
Level 1	The first level of two factor authentication mode (Security Questions, One Time Password , Soft Token, Push Notification based 2FA) set for the transaction type. The options are: • None • Security Question • One Time Password • Soft Token • Push Notification
Number of Question	Number of security questions to be asked from user at level 1 authentication. This field appears only if the **Security Question** option is selected as the **Authentication** mode.
Level 2	The second level of two factor authentication mode (Security Questions, One Time Password , Soft Token, Push Notification based 2FA) set for the transaction type. The options are: • None • Security Question • One Time Password • Soft Token • Push Notification
Number of Question	Number of security questions to be asked at level 2 authentication. This field appears only if the **Security Question** option is selected as the **Authentication** mode.

5. In **Transactions** section, in **Level 1** of authentication select the appropriate option.
   a. If user selects **Security Question** option:
6. In the **Number of questions** field enter the number of security questions to be asked.
7. In **Transactions** section, in **Level 2** of authentication select the appropriate option.
   a. If user selects **Security Question** option:
8. In the **Number of questions** field enter the number of security questions to be asked.

Note: Click **Apply to all** to apply the same kind of level 1 & level 2 authentication for all transaction types.

9. Click **Save** to save the changes made.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to go back to previous screen.
10. The **Authentication Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Edit** to make the changes if any.
    The **Authentication – Edit** screen with values in editable form screen appears.
    OR
    Click **Cancel** to cancel the operation and navigate back to ‘**Dashboard**’.
11. The success message of Authentication setup appears along with the transaction reference number.
    Click **OK** to complete the transaction and navigate back to ‘**Dashboard**’.

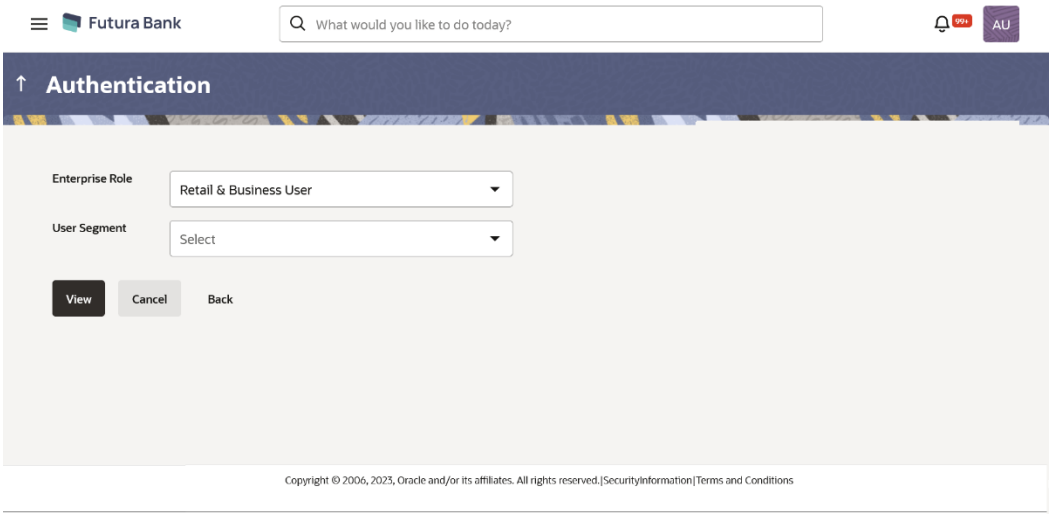
37.3 Authentication - Create

System Administrator can create authentication maintenance if the maintenance is not available.

To create the authentication setup for user segment:

1. From the **Enterprise Role** list, select the appropriate role.
2. From the **User Segment** list select the user segment (if applicable)

Authentication Setup



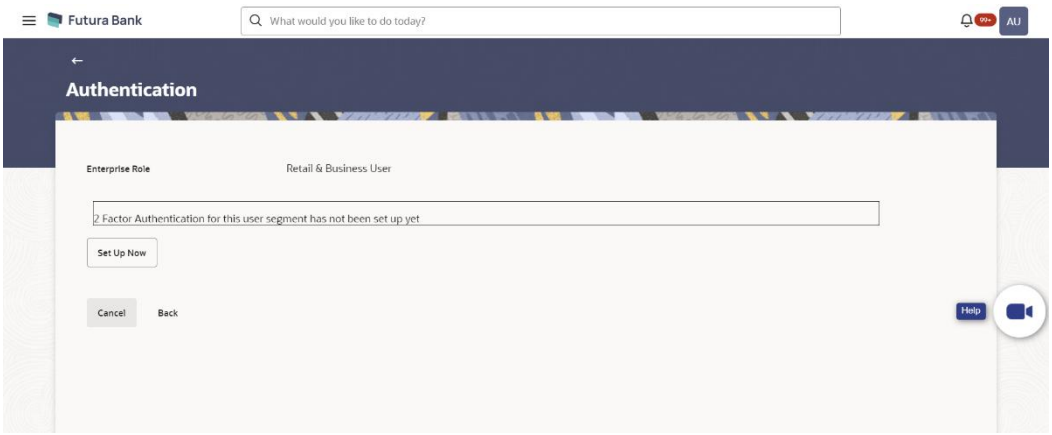
Field Description

Field Name	Description
Enterprise Role	The enterprise role for which the 2 Factor Authentication is set-up.
User Segment	The user segments maintained by the Bank. The options are: • Retail User • Corporate User

3. Click **Cancel** to can`cel the transaction.
   OR
   Click **View** to view the 2 Factor Authentications maintained for the user segment. The **Authentication - View** screen appears.

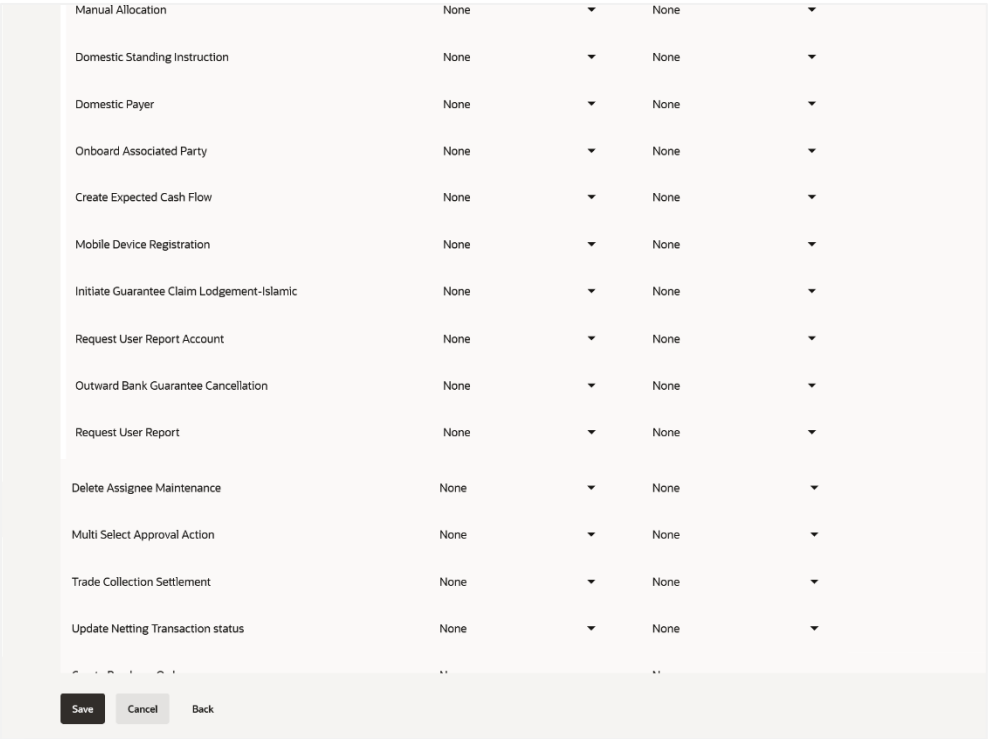
Note: If the existing maintenance is not available for selected user segment, message will be displayed "Authentication for this user segment has not been set up yet" with a setup now button.

Authentication - Create



4. Click **Set up now** to create new 2Factor Authentication. The Authentication - Create screen appears.

Futura Bank
What would you like to do today?
AU
Authentication
Enterprise Role
Retail & Business User
Transaction Type
Level 1
Level 2
Forgot Password
One Time Password
Time Based Soft Token
Apply to all
Forgot User ID
One Time Password
Security Question
No of Security Questions:
0
Edit Reconciliation/Allocation Rule
Prioritize/Non-prioritize Transaction
Create Periodic Payment - Berlin Open Banking
Create RD
Service Request - Debit Card Change
Bulk Payment - File Upload
Adhoc Domestic Payment
Mixed Payee - File Level Approval
Create Discount Offer
Cancel User Report
Initiate Islamic Transfer LC
Create MT101 Inbound Agreement Request
Update Additional Condition Maintenance
International Demand Draft - File Level Approval
Delete International Payee
Import Collection Modify
Update Demand Draft Payee
Initiate Import LC Amendment
Update Internal Payee
Demand Draft Payee - Record Level Approval
Initiate Letter of Credit
Delete External Account
International Payment
Mixed Payment - Record Level Approval
Update International Payee
Adhoc International Demand Draft
Loan and Finance Repayment
None



Field Description

Field Name	Description
Create	
Enterprise Role	The enterprise role for which the 2 Factor Authentication is set-up.
User Segment	The user segment for which the 2 Factor Authentication is set-up from. The options are: • Retail User • Corporate User
Transactions	
Transaction Type	The transaction type for which the 2 Factor Authentication is set-up.

Field Name	Description
Level 1	The first level of two factor authentication mode (Security Questions, One Time Password , Soft Token, Push Notification based 2FA) set for the transaction type. The options are: • None • Security Question • One Time Password(OTP) • Soft Token • Push Notification
Number of Question	Number of security questions to be asked from user at level 1 authentication. This field appears only if the **Security Question** option is selected as the **Authentication** mode.
Level 2	The second level of two factor authentication mode (Security Questions, One Time Password , Soft Token, Push Notification based 2FA) set for the transaction type. The options are: • None • Security Question • One Time Password(OTP) • Soft Token • Push Notification
Number of Question	Number of security questions to be asked from user at level 2 authentication. This field appears only if the **Security Question** option is selected as the **Authentication** mode.

5. In **Transactions** section, in **Level 1** of authentication select the appropriate option.
   a. If user selects Security Question option: In the Number of questions field enter the number of security questions to be asked.
6. In **Transactions** section, in **Level 2** of authentication select the appropriate option.
   a. If user selects **Security Question** option: In the Number of questions field enter the number of security questions to be asked.

Note: Click **Apply to all** to apply the same kind of level 1 & level 2 authentications for all transaction types.

7. Click **Save** to save the changes made.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.

OR
Click **Back** to go back tom previous screen.

8. The **Authentication Create– Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to make the changes if any.
   The **Authentication – Edit** screen with values in editable form appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to '**Dashboard**'.
   The success message of Authentication setup appears along with the transaction reference number.
   Click **OK** to complete the transaction and navigate back to '**Dashboard**'.

FAQ

1. Can I also set the 2 Factor Authentication for transaction approval?

You don't have to set up separate 2 Factor Authentication for transaction approval. The 2 Factor Authentication set for transaction initiation will also applied for transaction approval as well.

2. When will the changes made in authentication maintenance be applied?

Changes made in the authentication maintenance will be effective from an immediate effect. This will be applicable to new transactions initiated as well as for transactions pending for approval post the changes are effective.

3. Is it mandatory to set authentication method at both the levels?

No, you may set 1 level authentication for specific transaction. This can be achieved by selecting specific authentication method at level 1 and by specifying 'None' option at level 2.

4. Can I set 'No additional authentication required' for specific transaction?

Yes, this can be achieved by selecting 'None' option at level1 and level 2. No additional authentication is required for transaction initiation and approval if both levels are set as 'None'.

5. Where can I define which security questions to be asked to the users?

A separate maintenance 'Manage Security Questions' is available to set the up the questions which are to be asked to the users as a part of authentication process.

6. **Is it mandatory to set up 2 factor authentication for a User Type and User Segment Combination**

No, User Segment is an optional field and is applicable for only for Retail type of users. If the Bank doesn't want to setup the authentication for a user segment, they can simply do it for each user type.

7. Can I set up this maintenance for each entity in case of a multi entity setup?

Yes, Authentication can be setup for each entity in case of a multi entity setup. User can select the entity from the entity selection drop-down available on the top right corner of the application to set up the maintenance.

8. If Push notifications is set a second factor authentication, then how will the user authenticate a transaction ?

User will receive a push notification on his registered device (mobile/wearable), he can click on the notification and authenticate and complete the transaction on the device where he has received the notification.

9. **If the user initiates a transaction form his mobile app and Push notification is set as the 2FA for that transaction , in this case where will he receive the push notification ?**

User will receive the notification on his registered device i.e. mobile or wearable. He can complete the transaction by clicking on the same on the mobile itself.

38. Security Questions Maintenance

This function allows the System Administrator to set up security questions, which will then be used as another layer of security (Over & above the Login credentials), before a user (Retail/ Corporate/ Administrator) can complete transactions through the internet channel.

Through the Manage Security Questions functionality, the administrator user can create and modify security questions. He / She can add the security questions, if required.

Features Supported In Application

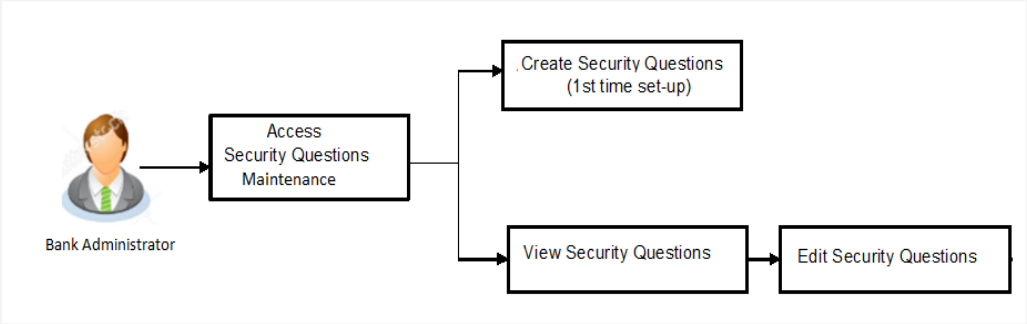
The following options are available to the administrator user as part of this maintenance:

- View Security Questions
- Edit Security Questions (Add new)
- Setup Security Questions (1st time setup)

Pre-requisites

- Transaction access is provided to System Administrator.

Workflow



How to reach here:

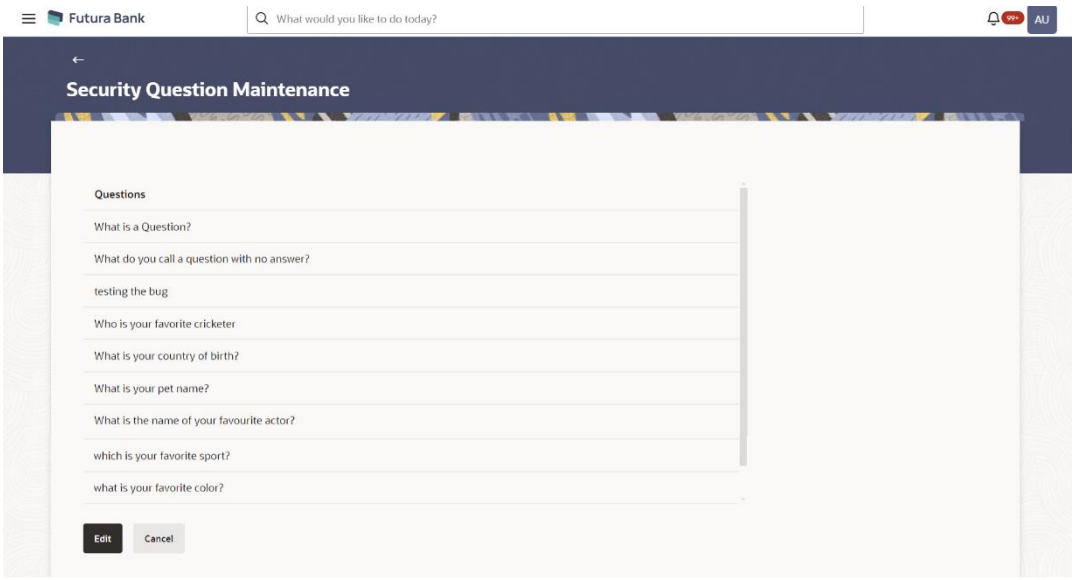
System Administrator Dashboard > Security> Security Questions Maintenance
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Security > Manage Security Questions

38.1 View Security Questions

On accessing ‘Manage Security Questions’ option, system displays the existing security questions already maintained if any.

To view the existing security questions maintenance:

Security Questions Maintenance - View



Field Description

Field Name	Description
View	
Questions	The list of security questions set for users, as an added layer of security.

Note: If the first-time maintenance is not already done, a message will be displayed "Security Questions has not been set up yet". With a button alongside – ‘Set up now’

1. Click **Edit** to update the set of security questions. An editable screen appears.
   OR
   Click **Cancel** to cancel the transaction.

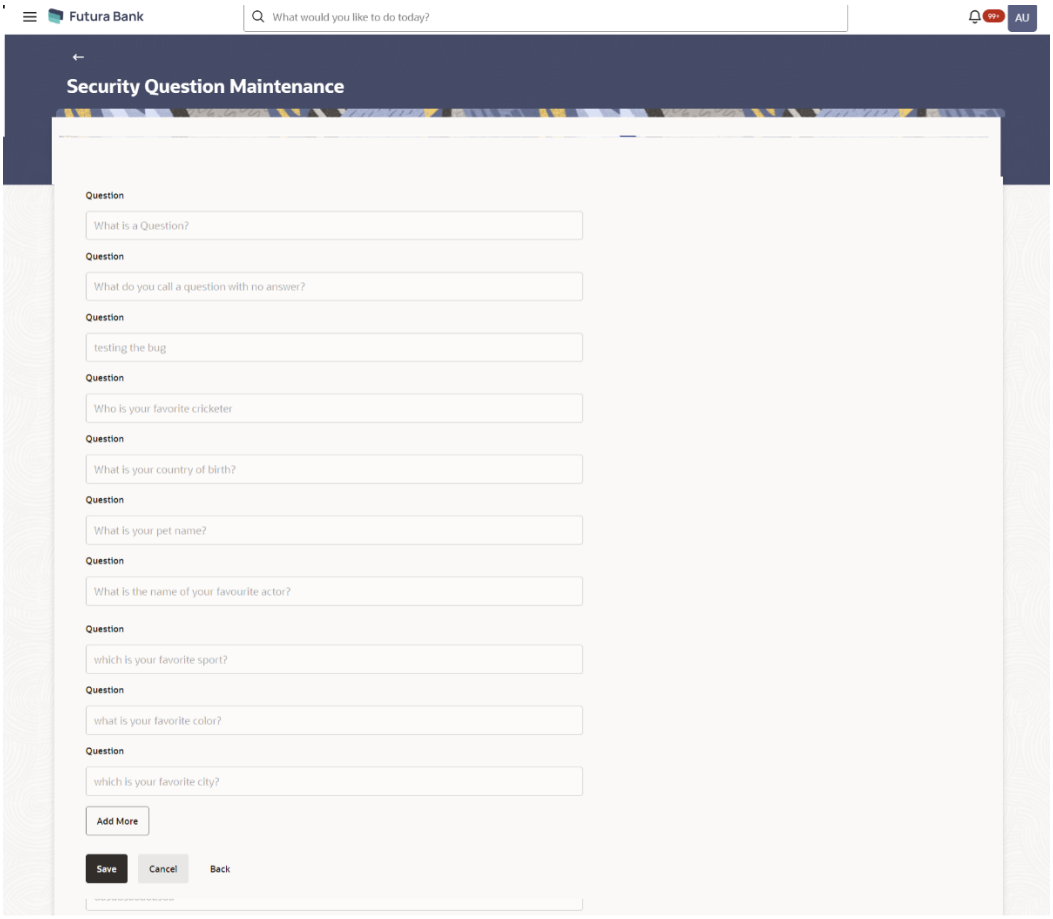
38.2 Security Questions Maintenance - Edit

System Administrator can modify existing maintenance for security questions. Administrator is allowed to add security questions but cannot delete the existing questions.

To edit the security questions set:

1. Click **View** to view the security questions already set. The **Security Questions Maintenance - View** screen appears.
2. **Click Edit**. **The Security Questions Maintenance – Edit** screen appears.

Security Questions Maintenance - Edit



Field Description

Field Name	Description
Edit	

Field Name	Description
Questions	
This section displays the security questions.	
Questions	The list of security questions.

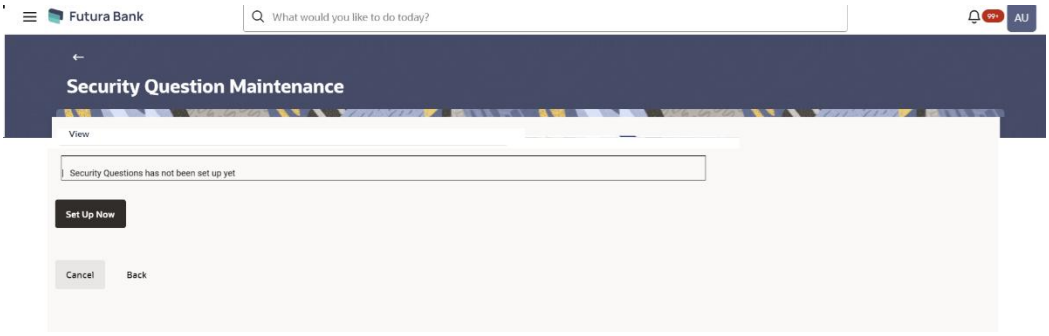
3. Click **Add More** to add more security questions.
   a. Type the new question to be added in the set.
4. Click **Confirm** to save the changes made.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to previous screen.
5. The **Security Questions Maintenance – Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to previous screen.
   The success message of security question setup appears along with the transaction reference number.
   Click **OK** to complete the transaction and navigate back to '**Dashboard**'.

38.3 Security Questions Maintenance - Create

As a part of first-time maintenance of Security Questions, the System Administrator can set-up security questions.

To set security questions:

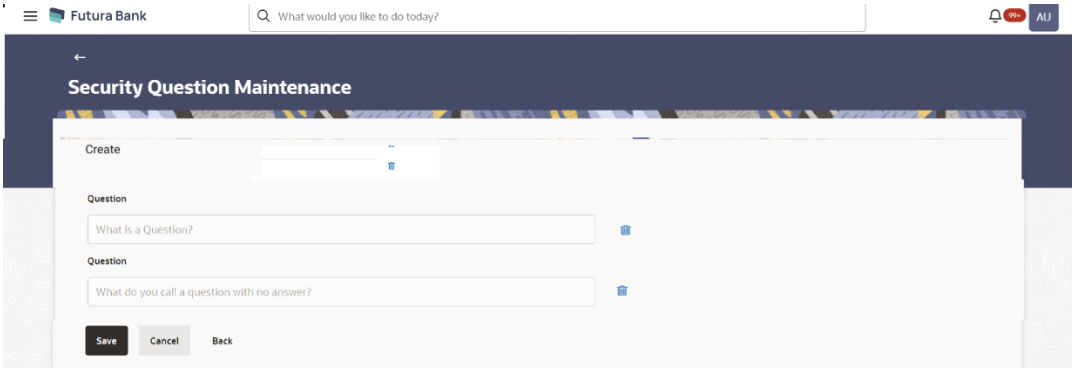
Security Question Maintenance - Setup



Note: Since the security question maintenance is not available, message will be displayed "Security Questions have not been set up yet". Alongside a button – "Set up now"

1. Click **Set up now** to set-up security questions. The **Security Questions Maintenance - Create** screen appears.

Security Questions Maintenance - Create



Field Description

Field Name	Description
Create	
Questions	
Questions	The list of security questions

2. Type the security question to be added.

Note: Click adjacent to question to delete the particular question.

3. Click **Add More** to add more security questions.
   a. Type the new question to be added in the set.
4. Click **Save** to save the changes made.
   OR
   Click **Cancel** to cancel the operation and navigate back to '**Dashboard**'.
   OR
   Click **Back** to go back tom previous screen.
5. The **Security Questions Maintenance – Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation and navigate back to '**Dashboard**'.
   OR
   Click **Back** to go back tom previous screen.
6. The success message of security question setup appears along with the transaction reference number.
   Click **OK** to complete the transaction and navigate back to '**Dashboard**'.

FAQ

1. **Can I delete the existing security questions?**

   No, you can add more questions, but cannot delete the existing questions.

2. **How many questions will be asked to the user as layer of security?**

   Number of questions to be asked shall be defined while defining ‘Authentication’ mode using ‘Authentication’ maintenance.

39. Security Keys

39.1 Password Encryption and Decryption with Public and Private Key Pairs

Encryption and decryption allow communication between two parties to disguise information. The sender encrypts information before sending it and the receiver decrypts the information after receiving it. While in transit, the information is encrypted to ensure that it is protected from an intruder.

Public and Private key pair helps to encrypt information that ensures sensitive data is protected during transmission. Whatever is encrypted with a Public Key can only be decrypted by its corresponding Private Key and vice versa.

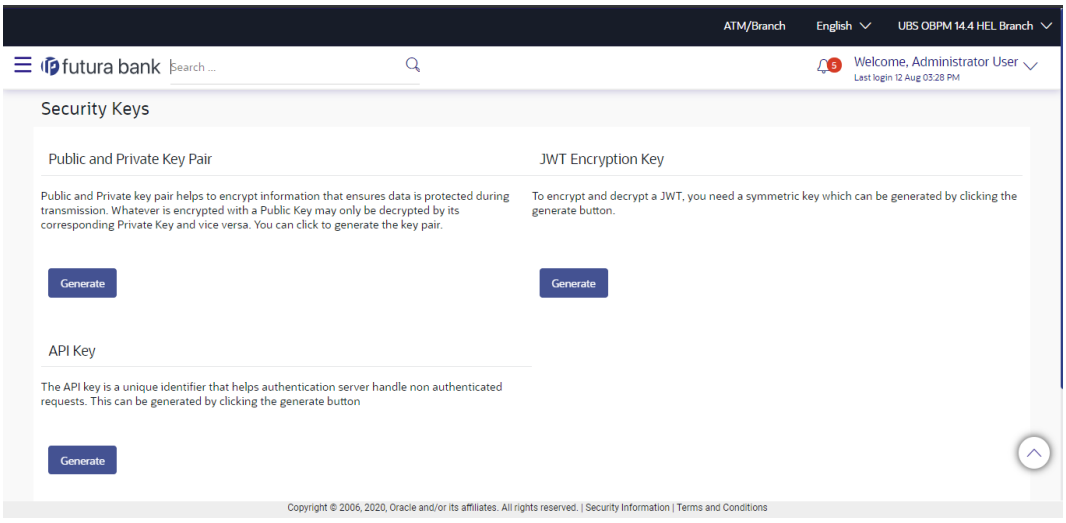
39.2 API Key

The API key is a unique identifier that helps authentication server handle non authenticated requests. This is required by asynchronous requests such as File upload, alerts, etc. to communicate with the authentication server. Hence, as a part of Day 1 activity, API Key should be mandatorily generated by clicking the "**Generate**" button.

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Security > Security Keys > API Key

API Key



Note : If you change the AES key connector password from Weblogic console, then you need to again generate the API key and take managed server restart.

39.3 JWT Encryption Key

A JSON web token is a JSON object to represent a set of information. On sign in, user is authenticated and JWT token is generated. This JWT is subsequently passed to make API calls.

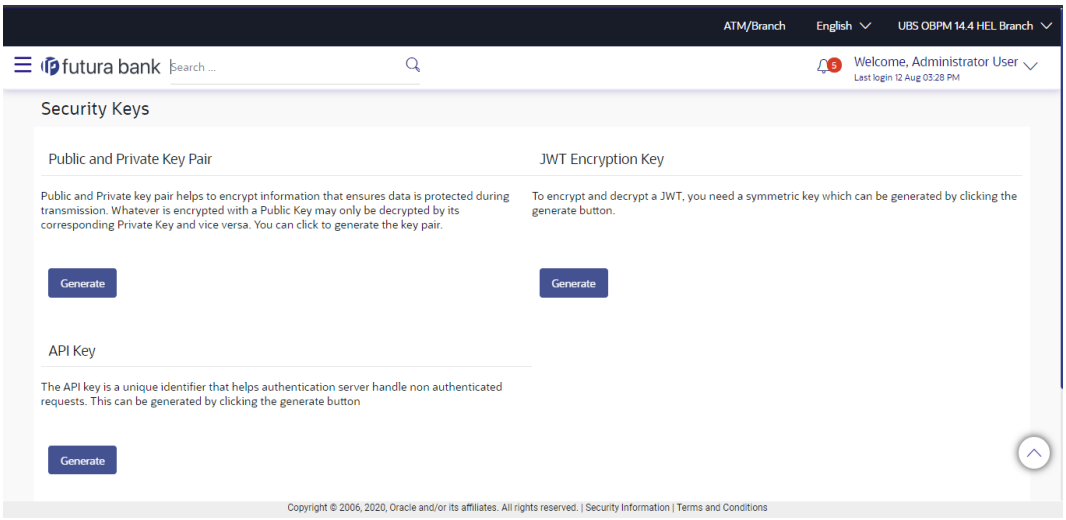
To keep sensitive information hidden from the bearer (client) or third parties, JWT should be encrypted.

A single key can be used to encrypt the data, if the JWT is encrypted with the key then the data can be decrypted using the same key.

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Security > Security Keys

Security Keys



To generate the security keys:

1. The default behaviour in the product will be no encryption for password as well as JWT.
2. If encryption needs to be enabled, then the system administrator should generate the respective keys.
3. Click **Generate** against the **Public and Private Key Pair**. System will generate public as well as private keys.
4. Click **Generate** against the **JWT Encryption Key**. System will generate the symmetric key for encryption.
5. Click **OK** to navigate back to dashboard

Note: The server will need to be restarted post key generation.

40. User Group - Subject Mapping

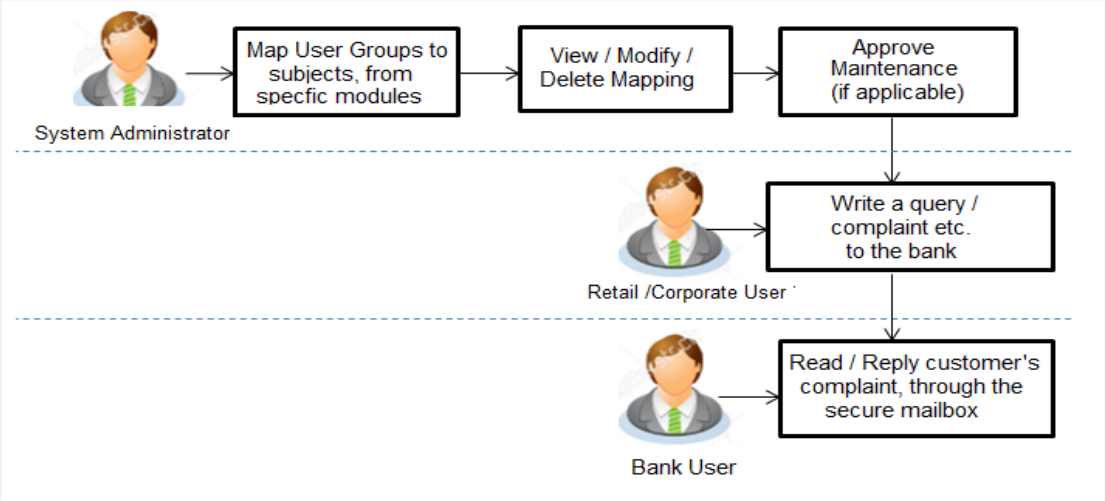
This maintenance facilitates mapping of subjects, to user groups in the bank, to streamline communication between the bank's users and its end customers.

Once User Groups are mapped to certain transactions or modules, users, in that group can reply to communication pertaining to the specific subject. The communication channel used is the bank's secure mailbox. For instance, employees in the Credit Card department of the bank will be able to reply to / address queries raised by customers who are overdue on their payments or who want to seek clarification on their monthly statement.

Pre-Requisites

- Transaction access is provided to System Administrator.
- Approval rule set up for System Administrator to perform the actions.
- Administrator user groups are maintained.
- Maintain applicable subjects, for each Module

Workflow



Features Supported In Application

- Search User Group - Subject Mapping
- Create User Group - Subject Mapping
- Modify User Group - Subject Mapping

How to reach here:

System/ Bank Administrator Dashboard > Communications > User Group Subject Mapping
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Communications > User Group Subject Mapping

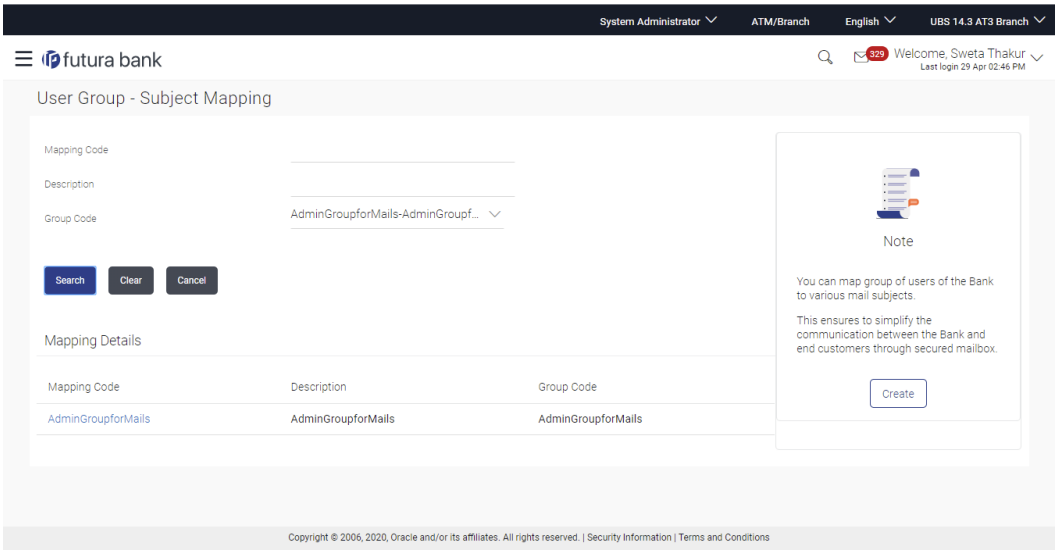
40.1 User Group - Subject Mapping - Search

User Group – subject mapping search option allows System Administrator to view the existing User Group - Subject Mapping.

To view User Group - Subject Mapping:

1. In the **Mapping Code** field, enter the user group - subject mapping code for which you want to view the details.
   OR
   In the **Description** field, enter the user group - subject mapping description for which you want to view the details.
   OR
   From the **Group Code** list, select the group code already maintained to view the details of the same. Click **Search**, display results based on search criteria.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction.

User Group - Subject Mapping - Search



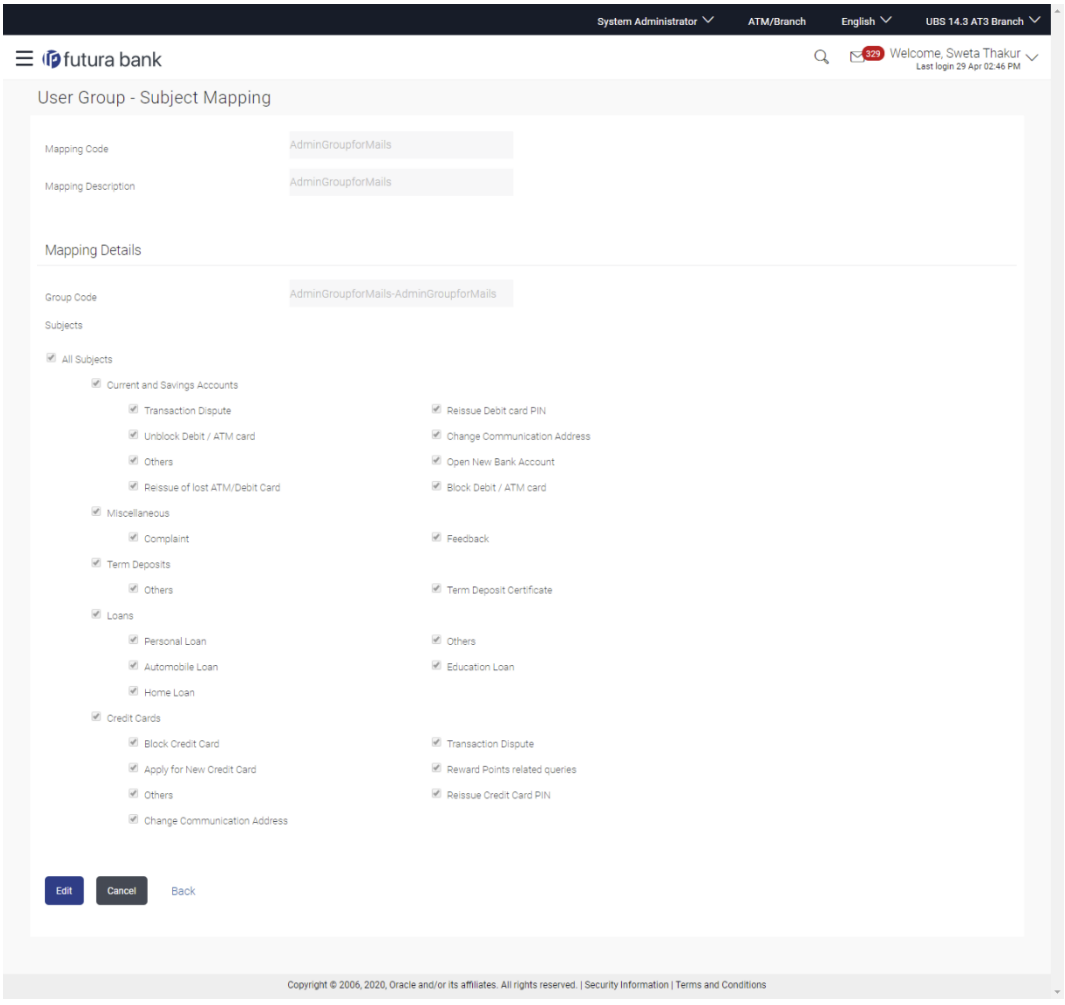
Field Description

Field Name	Description
Mapping Code	The user group - subject mapping code.
Description	The user group - subject mapping description.

Field Name	Description
Group Code	The group code to enquire about user group subject mapping, already maintained.

2. Click the **Mapping Code** for which you want to view the mapping details. The **User Group - Subject Mapping - View** screen displays the mapping of subject to the user group.

User Group - Subject Mapping - View



Field Description

Field Name	Description
Mapping Code	The user group - subject mapping code.

Field Name	Description
Description	The user group - subject mapping description.
Mapping Details	
Group Code	The group code assigned to user group subject mapping.
Subjects	The list of all subjects maintained.

Note:
1) All Subjects: if this is checked, then all subjects will be mapped with selected group code within the CASA, TD, Loans, Credit Cards modules.
2) List of Individual Subject: Module wise list of subjects will be available with check box against those. If this is checked, then individual subject is mapped with selected group code within the CASA, TD, Loans, Credit Cards and other modules.

3. Click **Edit** to edit the subject mapping details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.

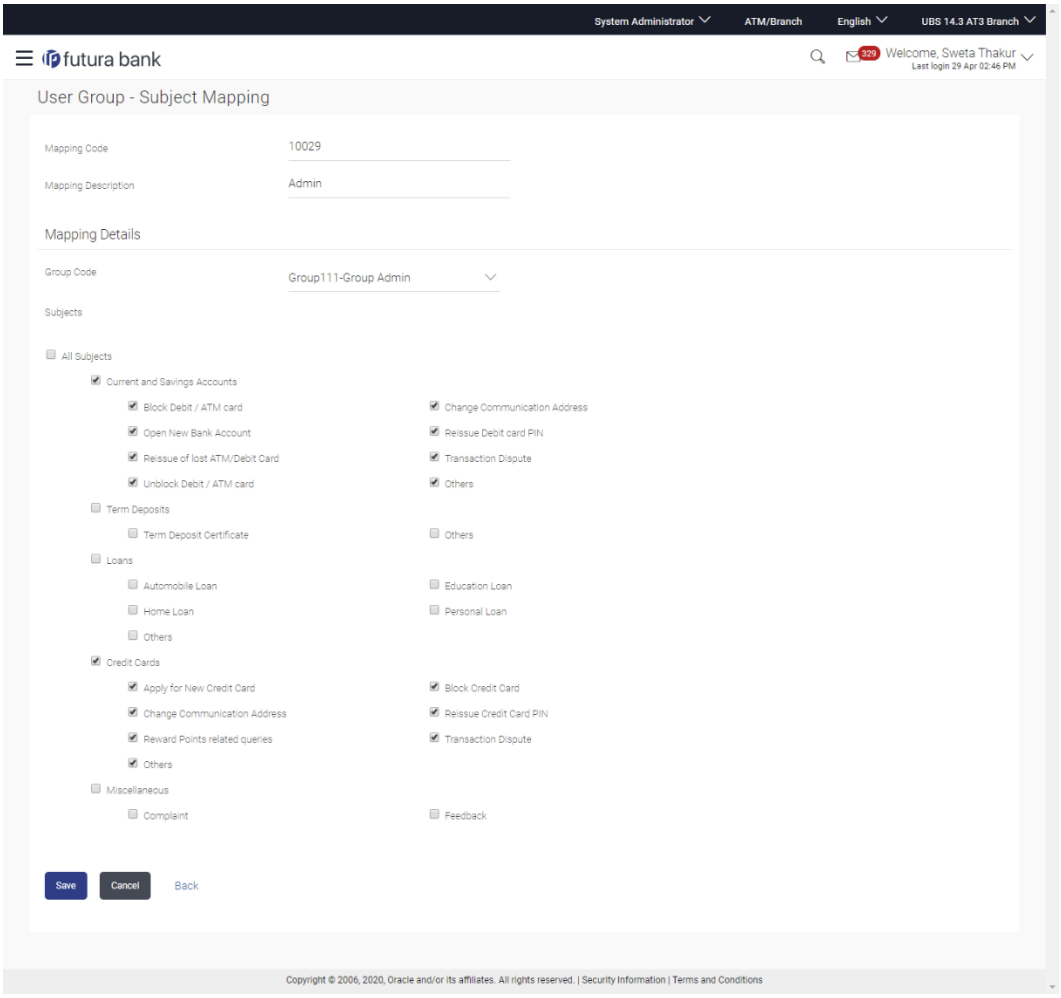
40.2 User Group - Subject Mapping - Create

Using User Group – Subject mapping - Create option, System Administrator can create the user group - subject mapping.

To create User Group - Subject Mapping:

1. Click **Create.**
   The **User Group - Subject Mapping - Create** screen appears.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction.

User Group - Subject Mapping - Create



Field Description

Field Name	Description
Mapping Code	The user group - subject mapping code.
Description	The user group - subject mapping description.
Mapping Details	
Group Code	The group code to create user group subject mapping.
Subjects	The list of all subjects maintained. **Note:** 1) All Subjects: if this is checked, then all subjects will be mapped with selected group code within the CASA, TD, Loans, and Credit Cards modules. 2) List of Individual Subject: Module wise list of subjects will be available with check box against those. If this is checked, then individual subject is mapped with selected group code within the CASA, TD, Loans, Credit Cards and other modules.

2. In the **Mapping Code** field, enter the user group - subject mapping code.
3. In the **Description** field, enter the user group - subject mapping description.
4. From the **Group Code** list, select the appropriate option.
5. Select the respective check boxes preceding the subject to be mapped.
   OR
   Select **All Subjects** check box, if you want to map all subjects.
6. Update the required details.
7. Click **Save** to save the modified details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
8. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Edit** to modify the details.
9. The success message of creation of user group - subject mapping along with the transaction reference number appears.
   Click **OK** to complete the transaction.

Note:
1) If the mapping setup requires an approval workflow, the maintenance will be initiated. Once approved by the required number of approvers, the mapping will be effected.
2) If the setup does not require an approval workflow or is self / auto approved, then the mapping will be effected immediately.

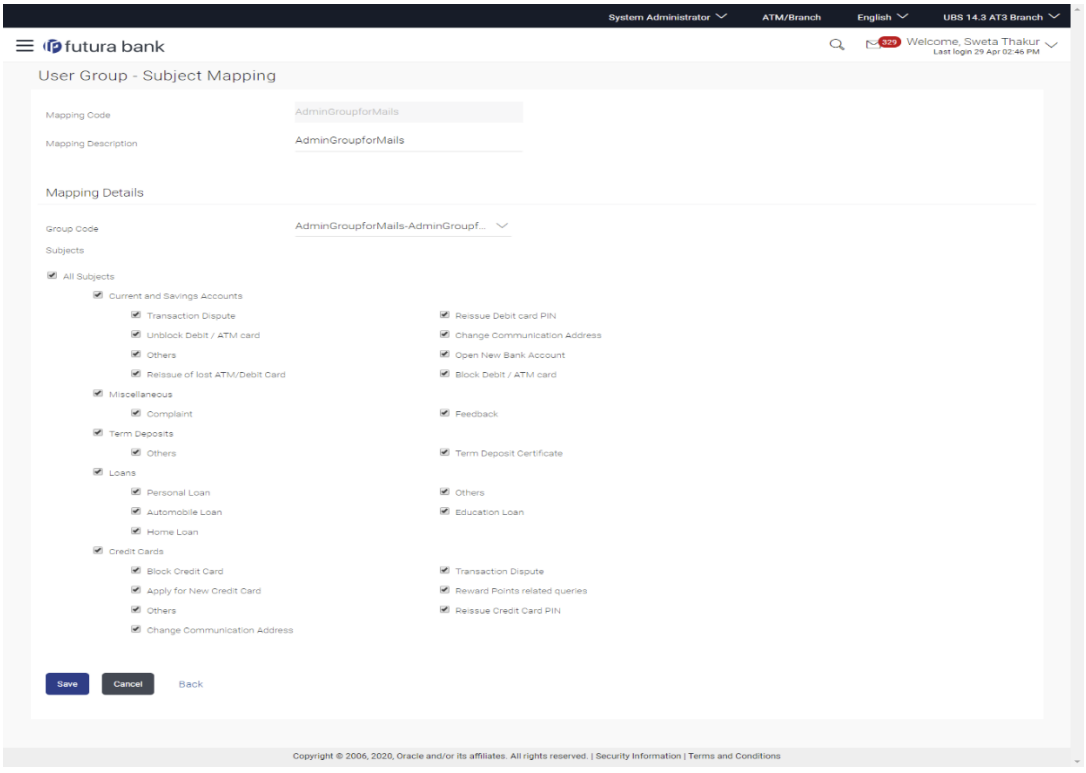
40.3 User Group - Subject Mapping - Modify

Using User Group – Subject Mapping - Modify option; System Administrator can edit the user group - subject mapping.

To edit the User Group - Subject Mapping:

1. In the **Mapping Code** field, enter the user group - subject mapping code for which you want to view the details.
   OR
   In the **Description** field, enter the user group - subject mapping description for which you want to view the details. OR
   From the **Group Code** list, select the group code already maintained to view the details of the same.
2. Click **Search to** display results based on search criteria.
3. Click the **Mapping Code** for which you want to view the mapping details. The **User Group - Subject Mapping - View** screen displays the mapping of subject to the user group.

User Group - Subject Mapping - Edit



Field Description

Field Name	Description
Mapping Code	The user group - subject mapping code.
Description	The user group - subject mapping description.
Mapping Details	
Group Code	The group code assigned to user group subject mapping.
Subjects	The list of all subjects maintained. **Note:** 1) All Subjects: if this is checked, then all subjects will be mapped with selected group code within the CASA, TD, Loans, and Credit Cards modules. 2) Individual Subject: if this is checked, then individual subject is mapped with selected group code within the CASA, TD, Loans, Credit Cards modules.

4. Select the respective check boxes preceding the subject to be mapped.
   OR
   Select **All Subjects** check box, if you want to map all subjects.
5. Update the required details.
6. Click **Save** to save the modified details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Edit** to modify the details.
8. The success message of update along with the transaction reference number appears. Click **OK** to complete the transaction.

Note:
1) If the mapping setup requires an approval workflow, the maintenance will be initiated. Once approved by the required number of approvers, the mapping will be effected.
2) If the setup does not require an approval workflow or is self / auto approved, then the mapping will be effected immediately.

FAQ

1. **If a user has been mapped to all subjects in the CASA module, what does it mean?**

   If the bank user is mapped to all subjects in CASA, he will be able to receive and reply to the business users on those CASA subjects.

2. **How does this maintenance help the bank and its customers?**

   This set-up is a way to allow or restrict access, to the users of the bank. This enables a secure communication channel between the bank and its end customers.

3. **I am an employee of the bank, and I belong to the user group that is mapped to all Term Deposits subjects. Can I initiate an email and send it to the customer?**

   No, you cannot initiate a correspondence with a customer, you can only reply to his queries on Term Deposits, through the mailbox.

41. Alert Templates

This option allows the System Administrator to define required parameters for each alert that is to be sent to the banks internal (Administrators) and external users (Business users). User can define the alert messages to be sent to different recipients on different channels. Also the type of alert Mandatory or subscribed can be defined by the user for each event.

Application also supports actionable alerts. Actionable alerts help user taking an action on the alert message received so that he/she does not have to navigate to the respective transaction manually to take specific action on the message. These alerts can be defined for any of the delivery mode i.e. email, SMS, push notification and on screen.

Note: If both Retail and Business parties are mapped to a user, then the alerts behavior will be as below-
1) For the transactions done in a Retail Party, alert will be sent to the user's contact information available in the respective core banking application.
2) For the transactions done in a Business Party, alert will be sent to the user's contact information available at the user level in Digital Banking.

Factory shipped Actionable Alerts:

Corporate Approval – User will be able to click on the link available in the alert and he or she will be redirected to transaction approval page.

Pre-Requisites

- Transaction access is provided to System Administrator.
- Approval rule set up for System Administrator to perform the actions.
- Various events are maintained

Features Supported In Application

The features available to System Administrator users in the application:

- View alert templates already maintained
- Create a new alert template
- Edit an alert template
- Delete an alert template

How to reach here:

System Administrator Dashboard > Communications > Alert Templates
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Communications > Alert Templates
OR
Search bar > Communications – Alert Templates

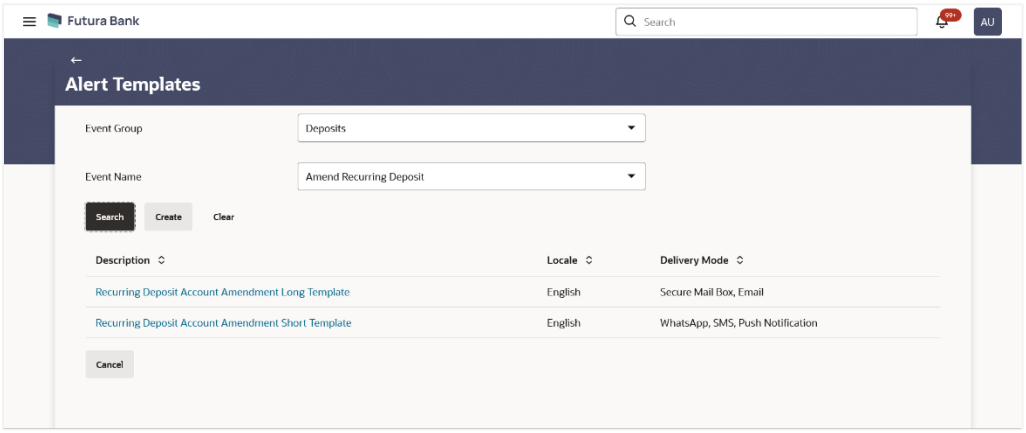
41.1 View Alert Template

Using this option, System Administrator can search and view the details of any alert templates maintained based on the search parameters. If the search parameters are not specified, records of all the alerts maintained in the application are displayed (i.e. a blank search is allowed).

To view alert templates:

1. From the **Event Group** list, select the appropriate option whose alert templates you to view.
2. From the **Event Name** list, select the event, for which one wants to view the alert templates maintained.
3. Click **Search**.
   The alerts maintained appear based on the entered search parameters.
   OR
   Click **Create** to create new alert template.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction.

Alert Templates - Search

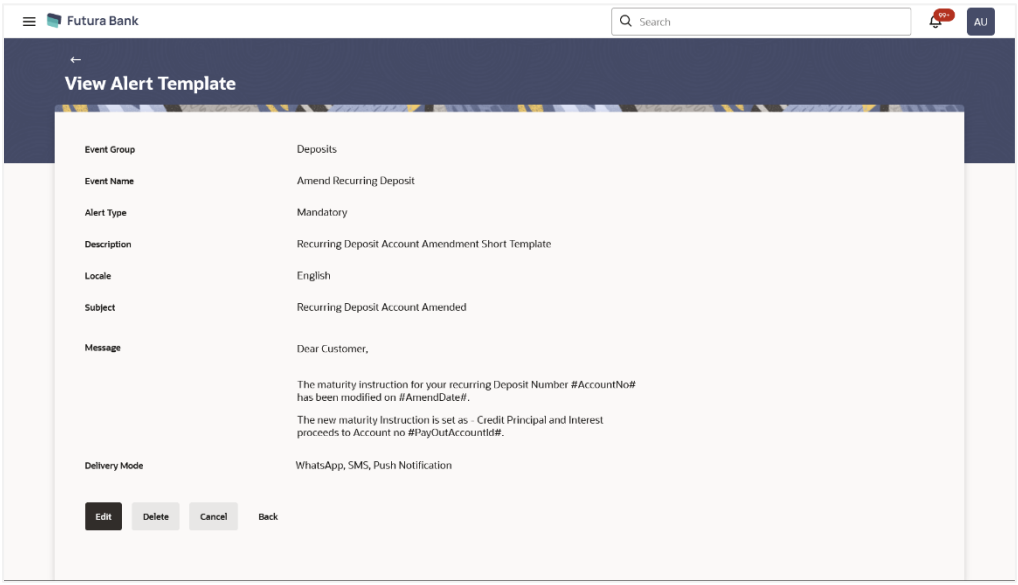


Field Description

Field Name	Description
Event Group	Name of the event for which alert is maintained.
Event Name	The event activity associated with the alert based on the event group selection.
Search Results	
Description	The details about the alert template. Click on the link to view the details od the alert template.
Locale	Language in which the message is defined.
Delivery Mode	The delivery mode through which the alert is to be sent. The options are: • Secure Mail Box: Alert is sent as a message to customer's secured mail box (mailbox available within OBDX). • Email: alert is to be sent as an email • SMS: alert is to be sent as an SMS on the user’s mobile number • Push Notification: notifications are sent as a banner or pop-up message on the user’s mobile number • WhatsApp

4. To view the details of a specific alert template, click on the **Description** link, in the Search Results table. The **Alert Templates- View** screen with maintained details appears.

View Alert Template



Field Description

Field Name	Description
Event Group	Name of the event for which alert is maintained.
Event Name	The event activity associated with the alert based on the Module name selection.
Alert Type	The type of alert i.e. if the alert is a subscription based alert or is one that is sent by the bank by default (mandatory). The options are: • S: Subscribed • M: Mandatory (Bank Notification)
Description	The details about the alert template.
Locale	Language in which the message is defined.
Subject	The subject as specified in the template.
Message	
Subject	The subject as specified in the template.
Message	The content of the template.

Field Name	Description
Delivery Mode	The delivery mode through which the alert is to be sent. The options are: • Secure Mail Box: Alert is sent as a message to customer's secured mail box (mailbox available within OBDX). • Email: alert is to be sent as an email • SMS: alert is to be sent as an SMS on the user's mobile number • Push Notification: notifications are sent as a banner or pop-up message on the user's mobile number • WhatsApp

5. Click **Edit** to edit the alerts details.
   OR
   Click **Delete** to delete the alert. (Only non-mandatory alerts can be deleted).
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.

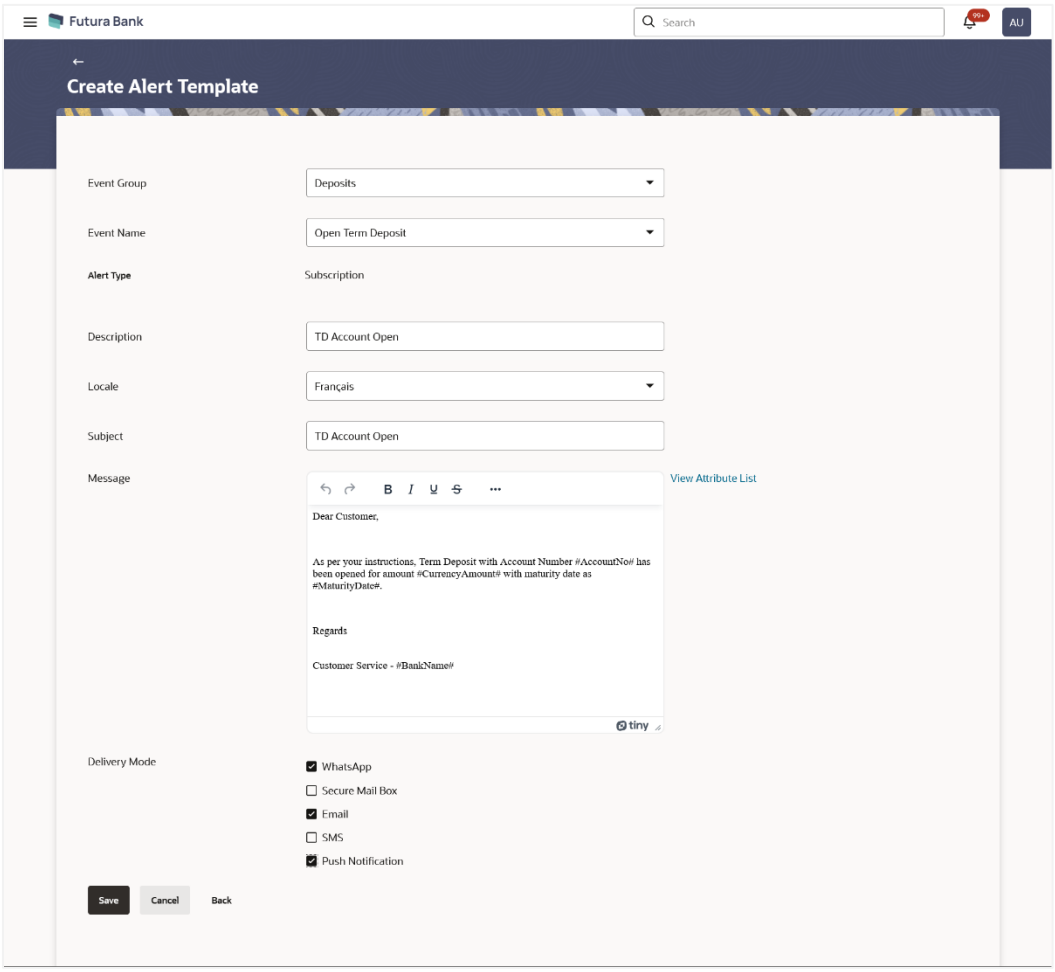
41.2 Create Alert Template

Using this option, the System Administrator defines the alert templates. User has to select the module-event combination for which the alert needs to be maintained. Further user has to select the recipients for whom the alerts need to be sent on an event.

To create an alert template:

1. Navigate to the **Alert Templates** screen.
2. Click **Create** to create an alert. The **Alert Maintenance - Create** screen appears.

Create Alert Template



Field Description

Field Name	Description
Event Group	Name of the event for which alert is to be created.

Field Name	Description
	The options are: • Term Deposits • Current and Savings Account • Loan • Originations • Payments • Host • User Management • Back Office • File Upload • Approvals • Credit Card • PFM • Reports • Wallets
Event Name	The event activity associated with the alert based on the event group selection.
Description	The details about the alert template.
Locale	Language in which the message is to be defined.
Subject	The subject as specified in the template.
Message	The content of the template.
Delivery Mode	The delivery mode through which the alert is to be sent. The options are: • WhatsApp • Email: alert is to be sent as an email • SMS: alert is to be sent as an SMS on the user’s mobile number • Secure Mail Box: Alert is sent as a message to customer's secured mail box (mailbox available within OBDX). • Push Notification: notifications are sent as a banner or pop-up message on the user’s mobile number

Field Name	Description
	Note: For Push Notification alerts, user can define separate sound/notification tone for different notifications so that, there can be a clear differentiation in the tone between an update (related to an account) and promotions.
	Click on one or more of the delivery mode to enable the following fields

3. From the **Event Group** list, select the appropriate option for whom alert template you wish to create.
4. From the **Event Name** list, select the appropriate option which you want to create alert.
5. In the Description field. Enter the description for the alert template to be created..
6. From the **Locale** list, select the appropriate option.
7. In the **Subject** field, enter the subject for the alert template.
8. In the **Delivery Mode** field, select the appropriate option.
9. Click **Save** to save the details entered.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
10. The **Review** screen appears. Verify the details and click **Confirm**.
    OR
    Click **Back** to navigate back to previous screen..
    OR
    Click **Cancel** to cancel the transaction.
11. The success message appears. Click **OK** to complete the transaction.

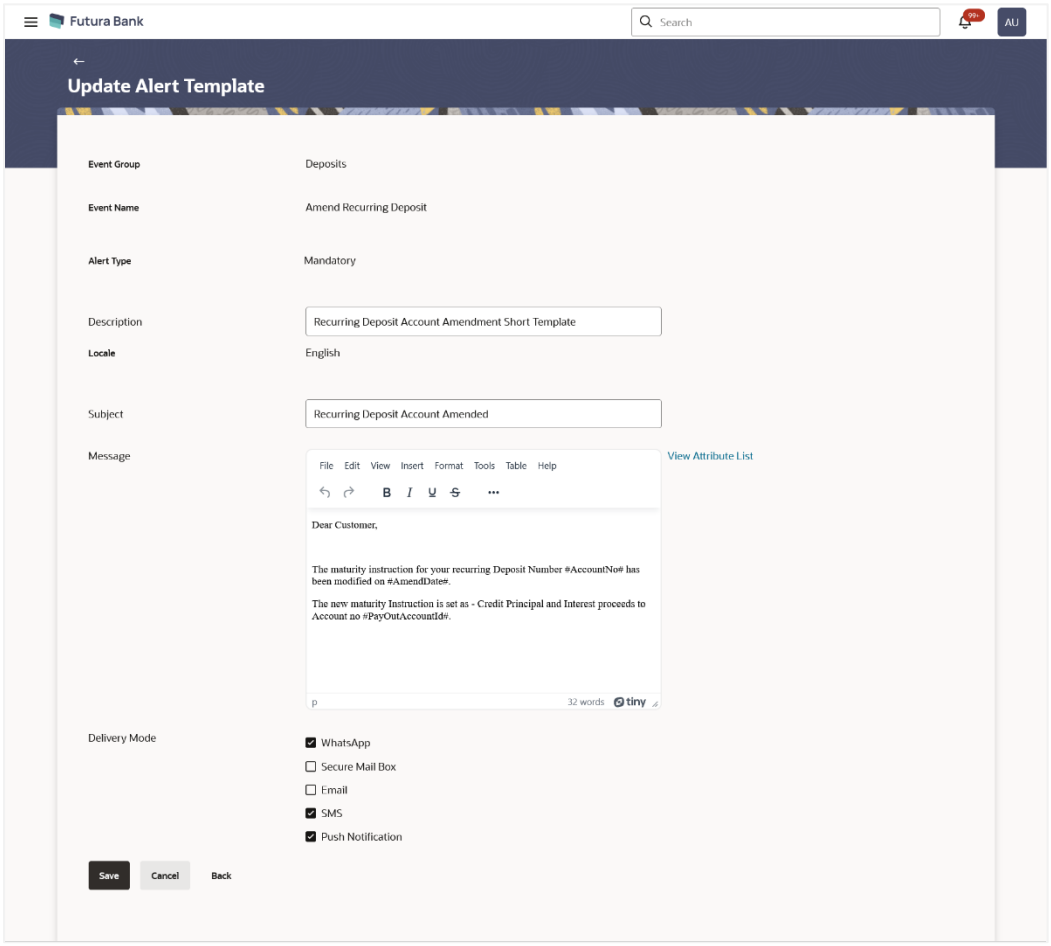
41.3 Update Alert Template

Using this option, System Administrator can edit the details of selected alert template defined in the application.

To modify an alert:

1. Enter the search criteria, and click **Search**.
   The alert templates maintained appear based on the entered search parameters.
   OR
   Click **Create** to create new alert template.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction.
2. Click on alert template description link whose details you want to modify. The **Alert Template- View** screen with maintained details appears.
3. Click **Edit** to edit the alert template details. The **Update Alert Template** screen appears.

Update Alert Template



4. Update the required fields.

Note:Event Group, Event Name, Alert Type, and Locale fields are read only, and cannot be edited.

5. Click to enable / disable the delivery mode, by clicking the check box.
6. Click **Save** to update the changes. User will be directed to the **Update Alert Template - Review** page post necessary validations.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to make the changes if any. The **Update Alert Template** screen with values in editable form appears.
   OR
   Click **Cancel** to cancel the transaction.
8. The success message appears. Click **Done** to complete the transaction.

41.4 Delete Alert Template

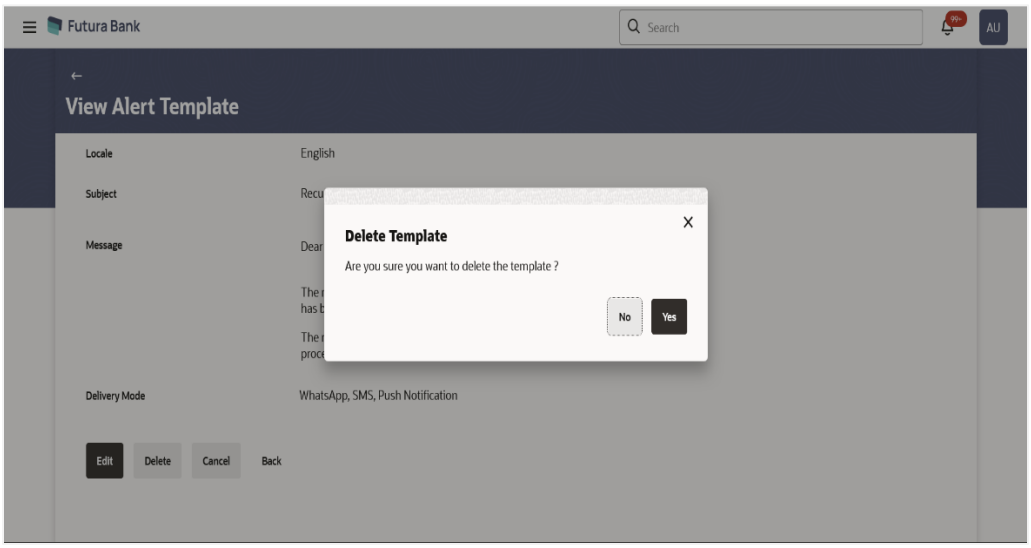
Using this option, you can search and delete an existing alert templates.

Note: The mandatory alerts cannot be deleted.

To delete an alert:

1. Repeat steps 1 to 2 of **Update Alert Template** section.
2. Click Delete to delete an alert template..
3. The **Delete Template popup** message appears, click **Yes**.
4. The **Alert Template** screen with the successful object deletion message appears. Click **OK** to complete the transaction.

Delete Alert Template



To view the list of events for **Alert Templates**, click here.

FAQ

1. **What is a significance of Mandatory and Subscribe types of alerts?**

   Recipients will get an alert by default for the alert types defined as Mandatory and will have to subscribe for those alerts for which the alert type is defined as 'Subscribe'.

2. **What is a reason for applying attribute masking?**

   The main reason for applying masking to a data field is to protect data that is classified as personal identifiable data, personal sensitive data or commercially sensitive data as a communication between the customer and Bank.

3. **Can I define the masking for data attribute available in subject?**

   No, data attribute masking can be defined only for the data available in the message body.

4. **Can I add an attribute masks for more the one data attribute for a specific recipient and channel?**

   Yes, you can add multiple attribute masks for different data attributes for a specific recipient and channel.

5. **Can I delete specific recipient added for an alert event in Alert Maintenance?**

   Yes, administrator can delete specific recipient mapped to an event.

6. **What happens to the in-transit transactions if I edit the alert maintenance for specific recipient?**

   An updated maintenance will be applicable for any new event performed after maintenance is saved successfully.

7. **Can the administrator define any of the existing alerts as an actionable alert by defining the Action ID and Action Text?**

   No, actionable alerts cannot be configured by the Administrator, these alerts are factory shipped or can be defined at the time of implementation. Administrator can only define the Action Text for and can enable/disable the actionable alert.

42. Mailers

Mailers are information or messages published by the Bank, to communicate about the Bank's Products, services and other information to its users. Bank may send mailers to announce a limited period promotional product rate, launch of a product or service, etc.

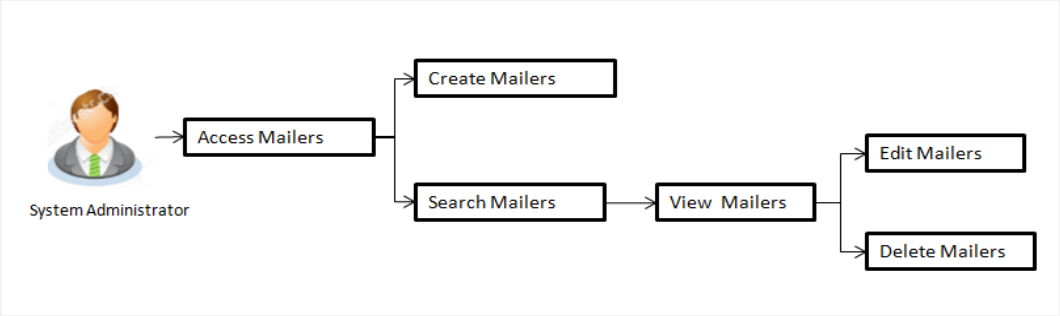
Using this option, the System Administrator creates Mailers which are sent to specific users, parties or user segments. Mailers can be customized to reach some or all users, to be sent now or on a specific date and time, in the future. Administrator can maintain mailers in all supported languages, to ensure effective communication with customers in their preferred language.

Note: Users can view mailer content (subject and body) in their currently logged-in language. If the administrator has not provided content in that language, the bank's default language will be used.

Pre-Requisites

- Transaction access is provided to System Administrator
- Approval rule set up for Administrator to perform the actions

Workflow



Features Supported In Application

The Mailers module supports following features:

- Search and View Mailers
- Create Mailers
- Edit Mailers (Only for Scheduled Mailers)
- Delete Mailers (Only for Scheduled Mailers)

How to reach here:

System/ Bank Administrator Dashboard > Communications > Mailers
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Communication > Mailers

42.1 Mailers - Search and View

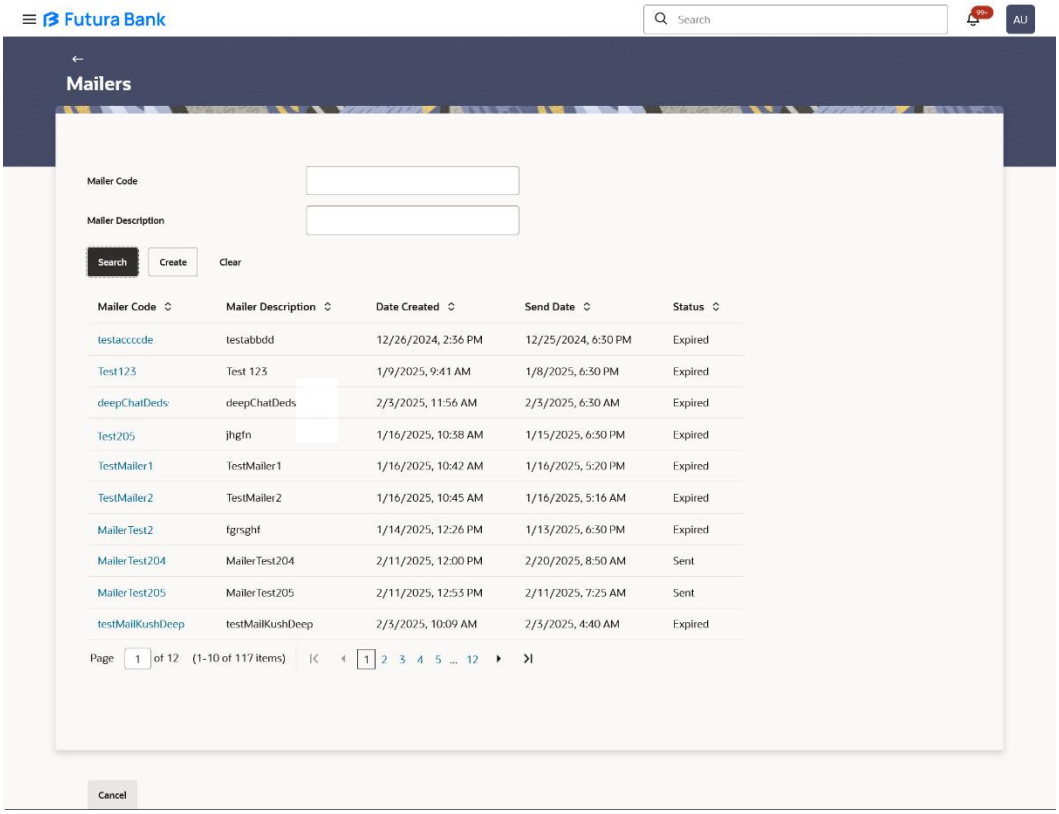
Using Mailers – search option, System Administrators can search and view the list of mailers created in the application. System Administrator enters the mailer code or mailer description to search the user, however blank search is also allowed.

The information will be displayed sorted by Date of creation.

To search the mailer:

1. In the **Mailer Code** field, enter the mailer code to view the mailer details.
   OR
   In the **Mailer Description** field, enter the mailer description to view the mailer details.
2. Click **Search**.
3. The search results appear on the **Mailers** screen.
   OR
   Click **Clear** if you want to reset the search parameters.
   OR
   Click **Cancel** if you want to cancel the transaction.

Mailers - Search



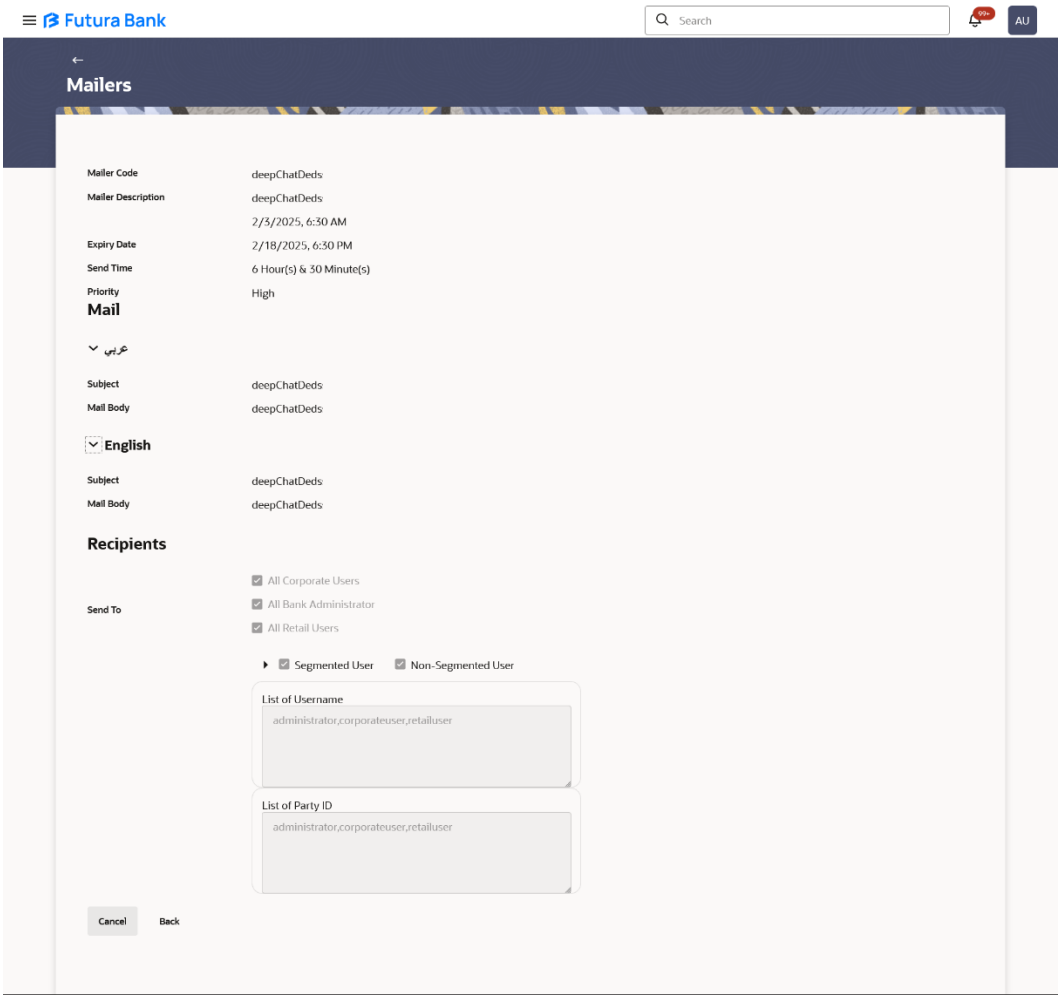
Field Description

Field Name	Description
Mailer Code	The unique key to identify the mailer.
Mailer Description	The description of the mailer corresponding to mailer code.
Search Results	
Mailer Code	The mailer code.
Mailer Description	The description of the mailer corresponding to mailer code.
Date Created	The date on which the mailer was created.
Send Date	The date on which mailer is sent.
Status	The status of the mailer - viz., scheduled, sent and expired.

To view the mailer details:

1. In the **Mailer - Search Results** section, click the **Mailer Code** link of the record for which you want to view the details.
   The search results appear on the **Mailers - View** screen appears.

Mailer - View



Field Description

Field Name	Description
Mail	
Mailer Code	The unique key to identify the mailer.
Mailer Description	The description of the mailer corresponding to the mailer code.
Send Date	The date and time on which the mailer was sent.
Expiry Date	The date and time on which the mailer will expire and will stop appearing in user's mailbox.

Field Name	Description
Send Time	The time on which the mailer was sent.
Priority	The priority of the mailer. The options can be: • Low • Medium • High
Subject	The subject of the mailer.
Mail Body	The content of the main body of the mailer.
Recipients	
Send To	The recipients of the mailer. The recipients can be: • All Corporate Users • All Bank Administrator • All Retail Users • Segmented Users • Non-Segmented Users • User IDs • Party IDs

2. Click **Edit** to edit the mailer.
   OR
   Click **Delete** the delete the mailer.
   OR
   Click **Cancel** the operation and navigate the user back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.

Note: The **Edit** and **Delete** option is available only for Mailers that have a status as '**Scheduled**'.

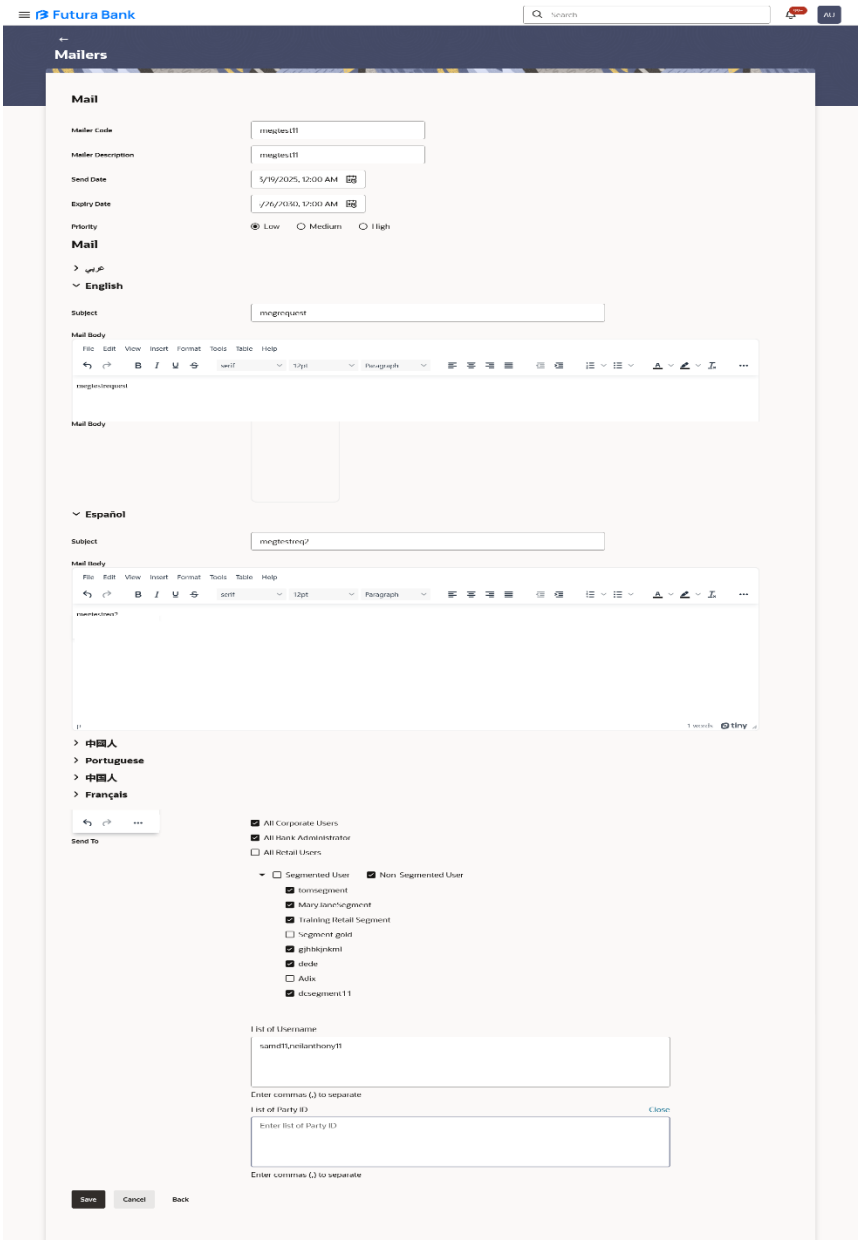
42.2 Mailers - Create

This function allows the System Administrator to create mailers. The System Administrator creates the content of the mailers, specifies the date - when a mailer is to be sent, priority of the mailer, and the recipients to whom the mailer needs to be sent.

To create a new mailer:

1. In the **Mailers** screen, click **Create**. The **Mailers - Create** screen appears.

Mailer - Create



Field Description

Field Name	Description
Mailer Code	Specify the unique key to identify the mailer.
Mailer Description	The description of the mailer corresponding to the mailer code.
Send Date	The desired date and time for sending the mailer.
Expiry Date	The date and time on which the mailer will expire and it will stop appearing in the user's mailbox.
Priority	The priority of the mailer. The options are: • Low • Medium • High
Mail	The following section displays the list supported languages in which Mailers can be maintain.
Language	Choose the preferred language in which mailer is to be defined. Drill down to add details of the mailer.
Subject	The subject of the mailer.
Mail Body	The content of the main body of the mailer.
Recipients	

Field Name	Description
Send To	The recipients of the mailer. The options are: • All Corporate Users • All Bank Administrator • All Retail Users • Segmented Users • Non-Segmented Users • List of User ID: This field is enabled, if you click the **Add List of User ID** button. • List of Party ID: This field is enabled, if you click the **Add List of Party ID** button.

2. In the **Mailer Code** field, enter the mailer id.
3. In the **Mailer Description** field, enter the mailer description.
4. From the **Send Date** list, select the appropriate date and time to send the mailer.
5. From the **Expiry Date** list, select the appropriate date and time on which the mailer will expire.
6. In the **Priority** field, select the priority to send the mailer.
7. Click on the **Language** for which you wish to maintain the mailer. The Content editor the mailer is displayed.
   b. In the **Subject** field, enter the appropriate subject for the mailer.
   c. In the **Mail Body** field, enter the appropriate content for the mailer.
8. To send the mailer, select the type of recipients from the **Send To** list.
   Click the ▶ against the Segmented Users/ Non Segmented Users field to view and select the desired user.
   OR
   Select the check box to select all the segmented users/ non segmented users.
   OR
   Click **Add List of User ID** and enter the user ids, if you want to add specific user ids as mailer recipients.
   OR
   Click **Add List of Party ID and enter the party ids**, if you want to add specific party ids as mailer recipients.
   OR
   Click **Save** to save the details.
   OR
   Click **Cancel** the operation and navigate the user back to 'Dashboard'.
   OR
   Click **Back** to navigate to previous screen.
9. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR

Click **Cancel** to cancel the transaction.
OR
Click **Back** to navigate to previous screen.

10. The success message of mailer creation appears along with the transaction reference number.
    Click **OK** to complete the transaction.

42.3 Mailers - Edit

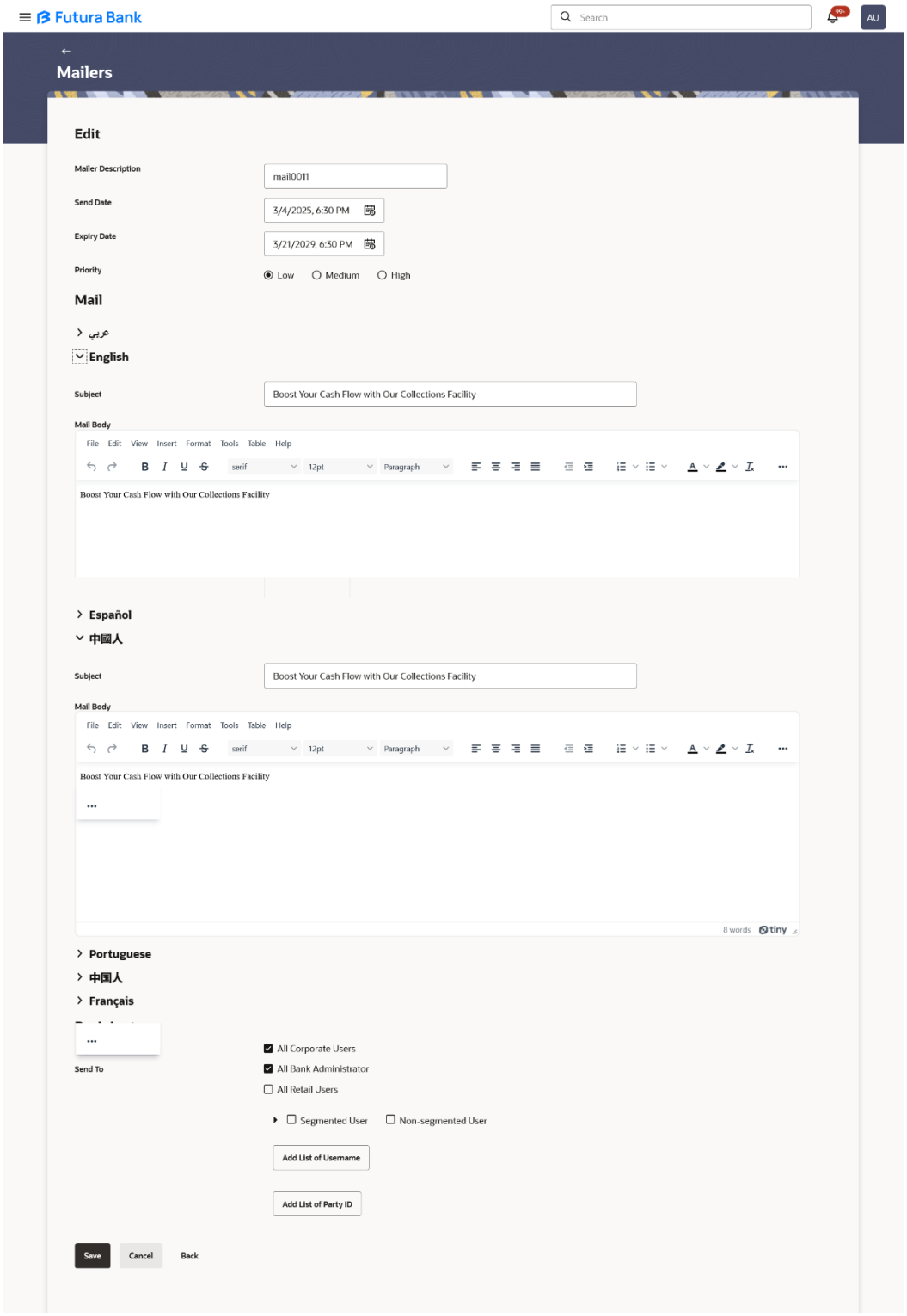
This function enables the System Administrator to edit the mailer details.

Note: This option is available only for Mailers, which have status as **Scheduled** (future dated).

To edit or update a mailer details:

1. Enter the search criteria, click **Search**.
   The search results appear on the **Mailers** screen.
2. In the **Mailer - Search Results** section, click the **Mailer Code** link of the record for which you want to view the details.
   The search results appear on the **Mailers - View** screen appears.
3. Click **Edit** to edit the mailer. The **Mailers - Edit** screen appears
   OR
   Click **Cancel** to cancel the operation and navigate the user back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.

Mailers - Edit


Futura Bank
Search
AU
Mailers
Edit
Mailer Description
mail0011
Send Date
3/4/2025, 6:30 PM
Expiry Date
3/21/2029, 6:30 PM
Priority
Low
Medium
High
Mail
عربي
English
Subject
Boost Your Cash Flow with Our Collections Facility
Mail Body
File Edit View Insert Format Tools Table Help
serif
12pt
Paragraph
Boost Your Cash Flow with Our Collections Facility
Español
中國人
Subject
Boost Your Cash Flow with Our Collections Facility
Mail Body
File Edit View Insert Format Tools Table Help
serif
12pt
Paragraph
Boost Your Cash Flow with Our Collections Facility
8 words
tiny
Portuguese
中国人
Français
Send To
All Corporate Users
All Bank Administrator
All Retail Users
Segmented User
Non-segmented User
Add List of Username
Add List of Party ID
Save
Cancel
Back

Field Description

Field Name	Description
Edit	
Mailer Code	The unique key to identify the mailer. This field is not editable.
Mailer Description	The description of the mailer corresponding to mailer code.
Send Date	The desired date and time for sending the mailer.
Expiry Date	The date and time on which the mailer will expire.
Priority	The priority of the mailer. The options are: • Low • Medium • High
Mail	The following section displays the list supported languages in which Mailers can be maintain.
Language	Choose the preferred language in which mailer is to be defined. Drill down to add details of the mailer.
Subject	The subject of the mailer.
Mail Body	The content for the mail body of the mailer.
Recipients	

Field Name	Description
Send To	The recipients of the mailer. The options are: • All Corporate Users • All Bank Administrator • All Retail Users • Segmented Users • Non-Segmented Users • List of User ID: This field is enabled, if you click the **Add List of User ID** button. • List of Party ID: This field is enabled, if you click the **Add List of Party ID** button.

4. View the defined values for fields, in an editable form.
5. Modify the required details.
6. Click **Save** to update the changes.
   OR
   Click **Cancel** to cancel the operation and navigate the user back to 'Dashboard'.
   OR
   Click **Back** to navigate to previous screen.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
8. The success message of mailer update appears along with the transaction reference number. Click **OK** to complete the transaction.

42.4 Mailers - Delete

Using this option, the System Administrator can delete the mailer.

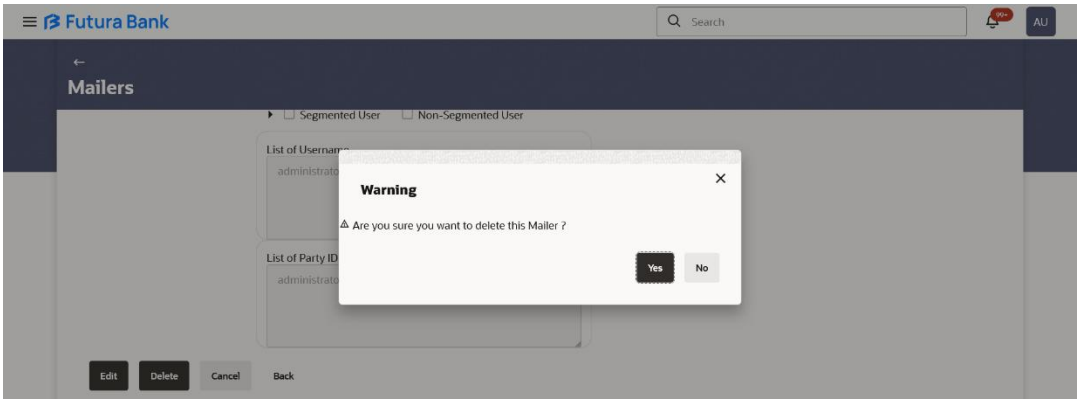
Note: This option is available only for Mailers, which have status as '**Scheduled**' (future dated).

To delete the mailer:

1. Enter the search criteria, click **Search**.
   The search results appear on the **Mailers** screen.

2. In the **Mailer - Search Results** section, click the **Mailer Code** link of the record for which you want to view the details.
   The search results appear on the **Mailers - View** screen appears.
3. Click **Delete**. The application prompt the System Administrator with a delete confirmation message with an option of **Yes** / **No**.

Mailers - Delete



4. Click **Yes** to continue.
   OR
   Click **No** to cancel the deletion process.
5. The screen with success message appears. Click **OK** to complete the transaction.

FAQ

1. Can I attach a file while creating a Mailer?

No, option to attach files is not supported.

2. Till which date I can see the mailers which are already sent to the customers?

You can view already sent mailers till the date, data is available in the system. This will be based on the Bank's purging policy.

3. Can I send mailers to specific customers?

Mailers can be sent to all the customers (Retail/corporate/Administrators), specific user segments or to specific user(s) by specifying the user IDs or party IDs.

4. Who will be the recipients of the mailers incase if mailers are targeted for specific party id(s)?

The users to whom the party ID is mapped as primary party will receive the mailers on scheduled date and time.

43. Account Aggregation

Account aggregation feature allows retail users to link their external bank accounts to OBDX and provides with an ability to view and access all their savings, term deposits and loan accounts information anytime, anywhere using single digital platform. The benefit of account aggregation is that retail users get a snapshot of all financial accounts while being able to easily retrieve account details, such as net balance available across all the current and savings accounts, recent transactions, etc. in one place. Using this feature, the user log on to the application to see all financial accounts, instead of log in to several accounts to tally up a financial overview, which saves time and effort of the user.

As a part of Account Aggregation module OBDX enables a retail user to access external bank accounts, and aggregate accounts with OBDX, the system administrator has to perform External Bank Maintenance.

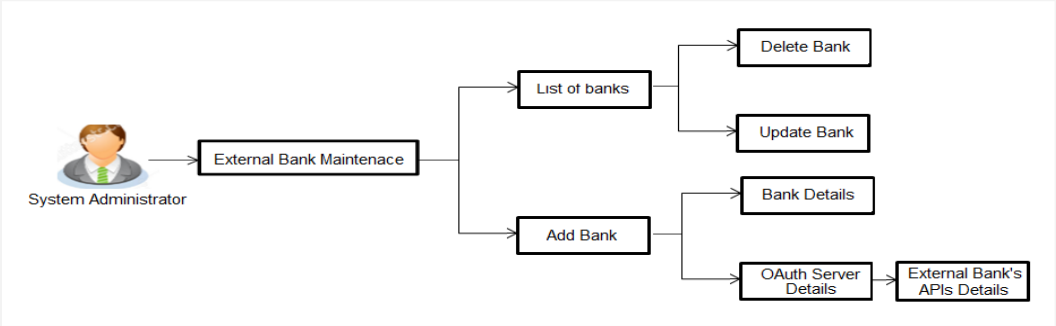
43.1 External Bank Maintenance

Using external bank maintenance, System Administrators can add an external bank. The external bank logo, address, URL and other details can be maintained. In addition to this, the authorization details can be captured, that will enable linking of OBDX with the external bank. Multiple external APIs can be saved, to facilitate access of data, which will then be available for the perusal of the OBDX customer.

Pre-Requisites

- Transaction access is provided to System Administrator
- Approval rule set up for System Administrator to perform the actions

Workflow



Features Supported In Application

This option allows the System Administrator to:

- View External Bank Details
- Add External Bank
- Update External Bank Details
- Delete External Bank

How to reach here:

System/ Bank Administrator Dashboard > Personal Finance > External Bank Maintenance
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Personal Financial Management > External Bank Maintenance

43.1.1 Search and View External Bank's Details

System Administrators can search and view the details of the external banks already maintained in the application.

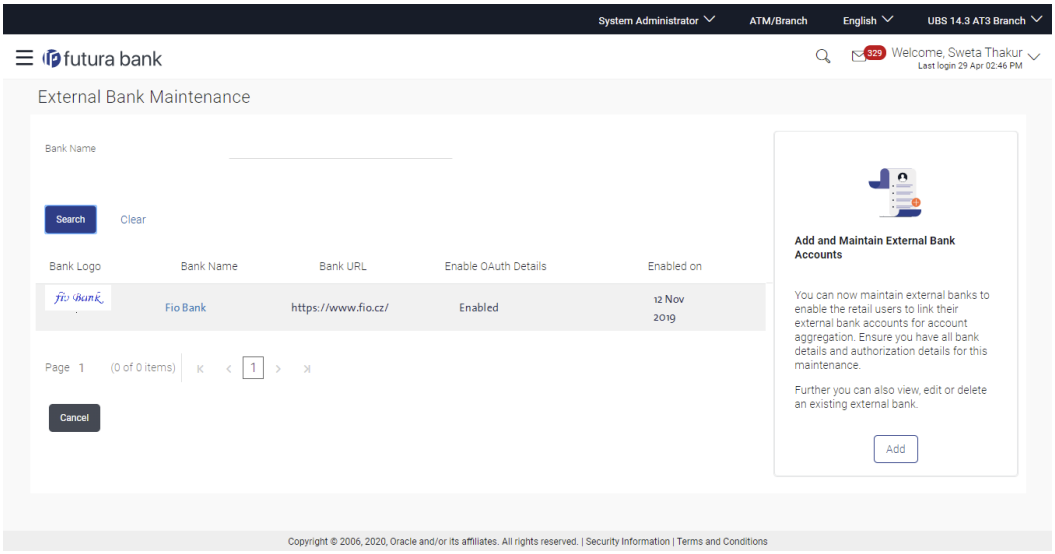
To view external bank's details:

1. In the **Bank Name** field, enter the bank name to search for a specific external bank.
2. Click **Search**.
   List of external banks matching search criteria appears in search summary section.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
   OR
   Click **Clear** to reset the details.

   OR

   Click **ADD to add new external bank.**

External Bank Maintenance - Search Result



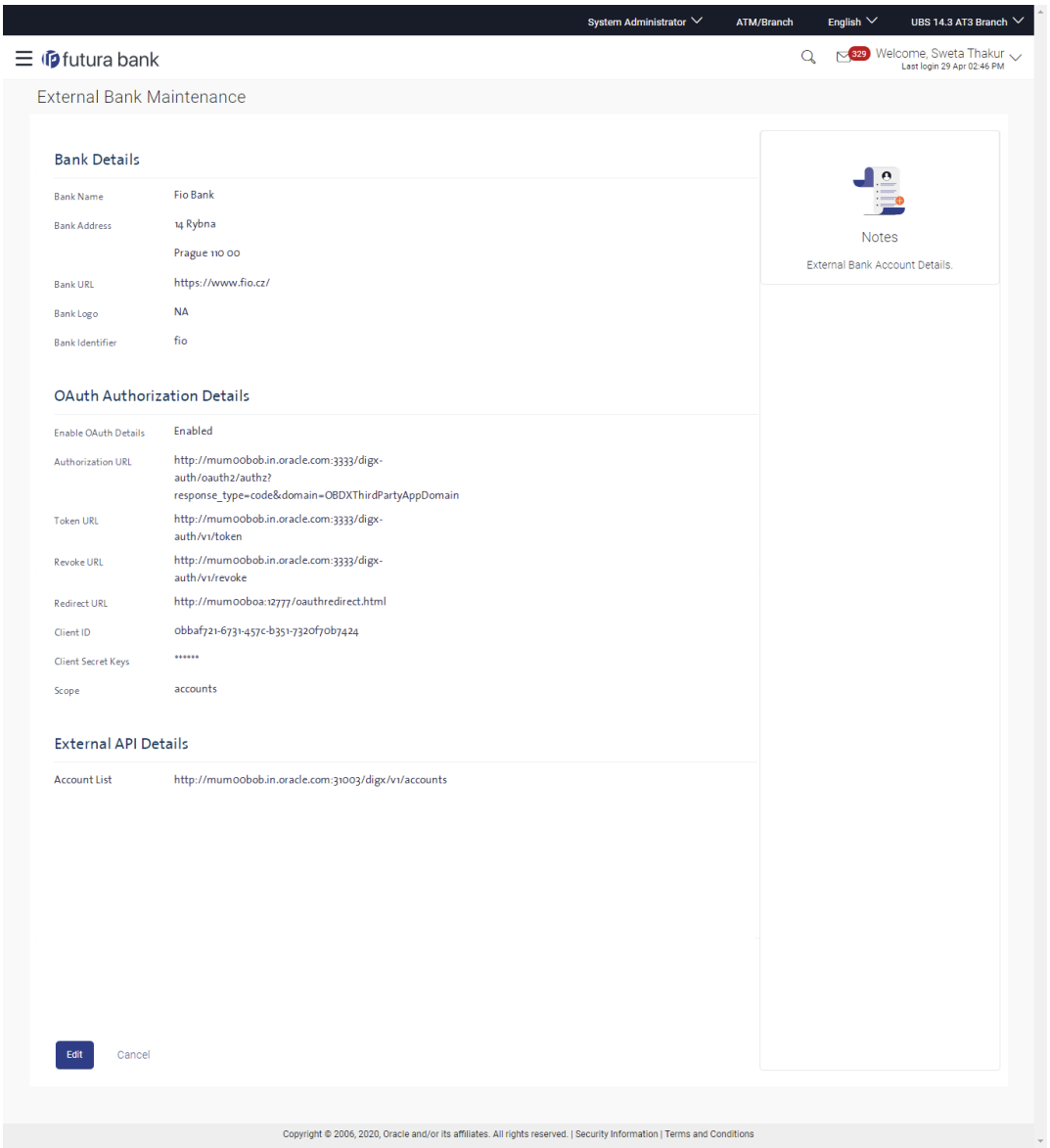
Field Description

Field Name	Description
Bank Logo	The external Bank's logo.
Bank Name	The name of the external bank maintained in OBDX.
Bank URL	The URL of the external bank maintained in OBDX.

Field Name	Description
Enable OAuth Details	The status of the external bank's authorization details, if enabled or disabled.
Enabled on	If the status of an external bank is enabled, then date and time on which the bank is enabled for customers.

3. Click **Bank Name** link on **External Bank Maintenance** screen.
   The bank details maintained appears on **External Bank Maintenance - View** screen.

External Bank Maintenance - View



Field Description

Field Name	Description
Bank Details	
Bank Name	The name of the external bank maintained in OBDX.
Bank Address	The address of the external bank maintained in OBDX.
Bank URL	The URL of the external bank maintained in OBDX.
Bank Logo	The external Bank's logo.
Bank Identifier	The external bank identifier.
OAuth Authorization Details	
Enable OAuth Details	Displays the authorization details status for the external bank i.e. whether to enable /disable.
Authorization URL	Displays the authorization url.
Token URL	Displays the Token url.
Revoke URL	Displays the Revoke url.
Redirect URL	Displays the Redirect url.
Client ID	Displays the Client ID.
Client Secret Keys	Displays the Client secret keys.
Scope	Displays the applicable scope(s) for the external bank.
External API Details	
External API's	Displays the category of external API's exchanged between the Banks.
API URL	Displays the API URL.

4. Click **Edit** to edit the external bank details.
   OR
   Click **Delete** to delete the external bank details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.

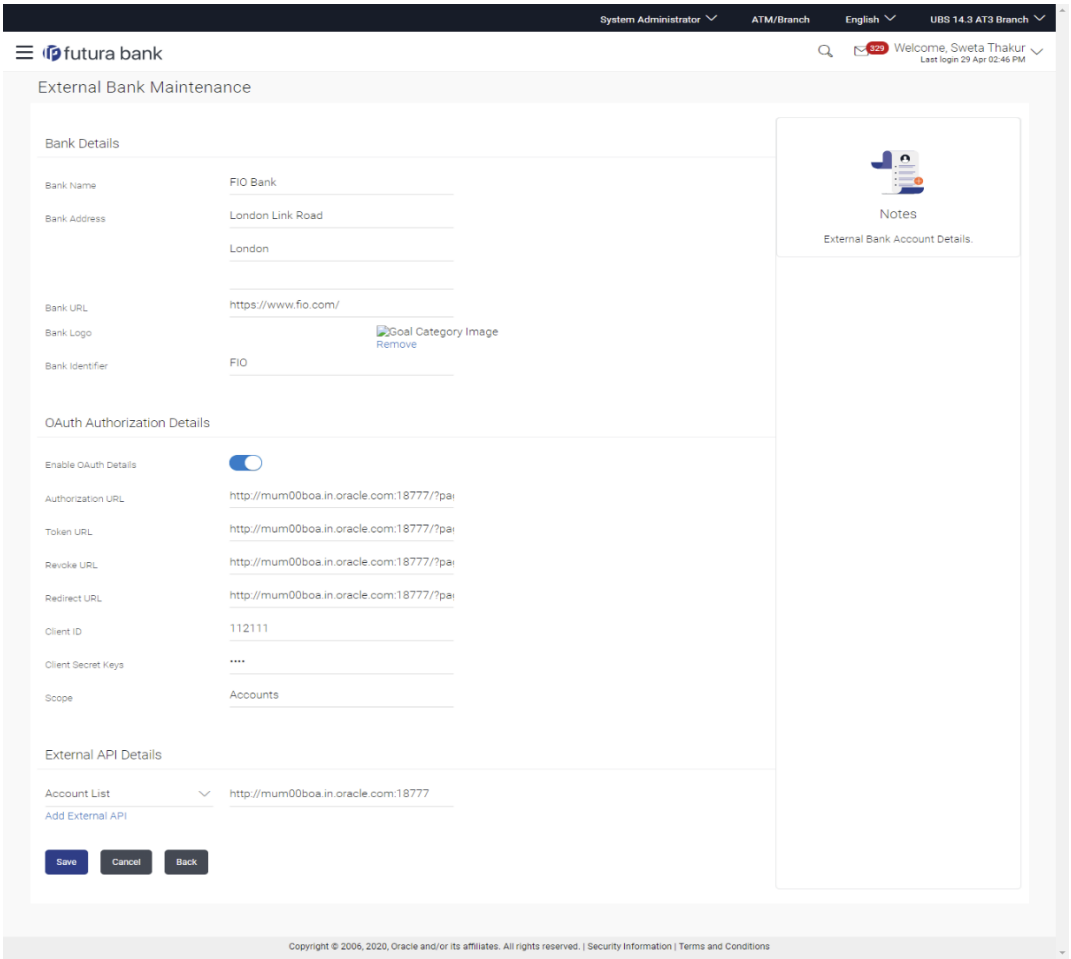
43.1.2 Add External Bank

System Administrators can add an external bank - so that it is available to the Retail User for account aggregation services (on successful authorization of this maintenance). System Administrators can add external bank details like Bank details, Bank Authorization details, multiple external APIs (to facilitate access of data between OBDX and the External Bank.)

To add external bank:

1. In the **External Bank Maintenance** screen, click **Add**. The **External Bank Maintenance - Create** screen appears.

External Bank Maintenance - Add



Field Description

Field Name	Description
Bank Details	
Bank Name	Specify the name of the external bank.
Bank Address	Enter address of the external bank.
Bank URL	Specify the URL of the external bank.
Bank Logo	Upload logo of the bank through browse and upload image option.
Bank Identifier	Enter the external bank identifier.
OAuth Authorization Details	
Enable OAuth Details	Select the authorization details status for the external bank i.e. whether to enable /disable.
Below fields is enabled only if the **Enable OAuth Details** field is **enable** under **OAuth Authorization Details** section	
Authorization URL	Specify the authorization URL.
Token URL	Specify the Token URL.
Revoke URL	Specify the Revoke url.
Redirect URL	Specify the Redirect url.
Client ID	Specify the Client ID.
Client Secret Keys	Specify the Client secret keys.
Scope	Specify the applicable scope(s) for the external bank.
External API Details	

Field Name	Description
External API's	Select the external API's category, to access data between OBDX and the External Bank. The External API could be to access the following information of the User's External Bank accounts: • Account List • Account Details • Account Summary • Account Activity
API URL	Specify the API URL.

2. In the **Bank Name** field, enter the external bank's name.
3. In the **Bank Address** field, enter the external bank's address.
4. In the **Bank URL** field, enter the external bank's url.
5. Click **Choose Files** or **Drag Files here**, browse and upload image of bank logo.
6. In the **Bank Identifier** field, enter the external bank's identifier.
7. Click the **Enable OAuth Details** toggle button to enable or disable the authorization details.

Note: **OAuth Authorization Details** are maintained for the external bank, if the status of the **Enable OAuth Details** field is enabled.

8. In the **Authorization URL** field, enter the external bank's authorization url.
9. In the **Token URL** field, enter the external bank's token url.
10. In the **Revoke URL** field, enter the external bank's revoke url.
11. In the **Redirect URL** field, enter the external bank's redirect url.
12. In the **Client ID** field, enter the external bank's client ID.
13. In the **Client Secret Keys** field, enter the external bank's client secret keys.
14. In the **Scope** field, enter the appropriate scope for the external bank.
15. From the **External APIs** list, select the external API's exchanged between the Banks in **External API Details** section.
16. Click **+ Add External API** to add more APIs.
    The list appears to select the APIs.
    a. From the drop-down list, select the appropriate option.
    b. In the **API URL** field, enter the API url.
    c. OR
    Click against the particular already added External API to delete it.

17. Click **Save** to update the changes.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to previous screen.
18. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to previous screen.
19. The success message of external bank details creation appears.
    Click **OK** to complete the transaction.

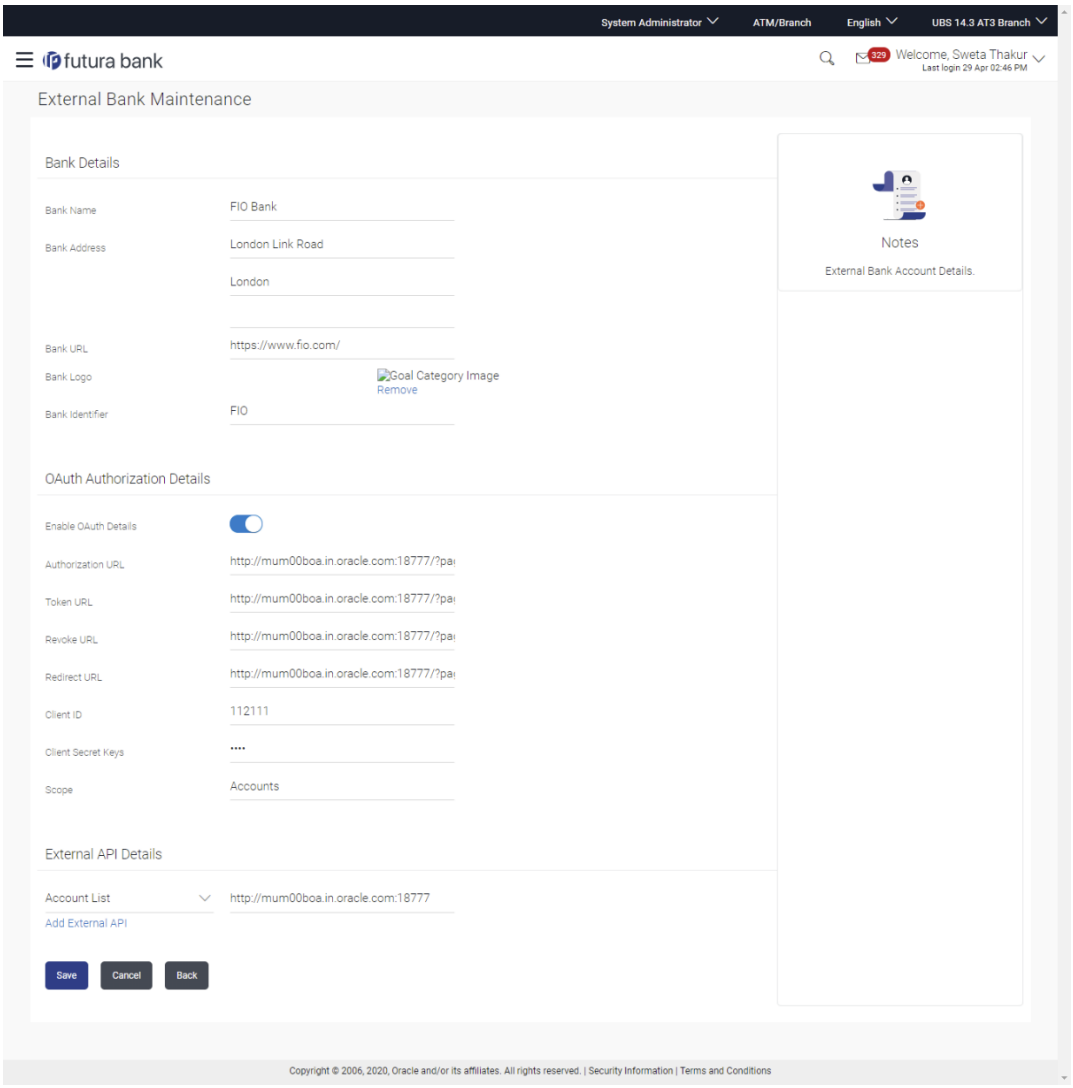
43.1.3 Update External Bank's Details

System Administrators can view and update the details of the external banks already maintained in the application. System Administrators can modify Bank details, Authorization details and External API information.

To edit External bank details:

1. In the **Bank Name** field, enter the bank name to search for the specific external bank.
2. Click **Search**.
   List of external banks matching the search criteria appears in search summary section.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to Dashboard.
   OR
   Click **Clear** to reset the details.
3. Click **Bank Name** link on **External Bank Maintenance** screen.
   The bank details maintained appears on **External Bank Maintenance - View** screen.
4. Click **Edit** to edit the external bank details. The **External Bank Maintenance - Edit** screen appears with values in editable form.

External Bank Maintenance - Edit



Field Description

Field Name	Description
Bank Details	
Bank Name	Displays the name of the external bank. This field is editable.
Bank Address	Displays an address of the external bank. This field is editable.

Field Name	Description
Bank URL	Displays the URL of the external bank. This field is editable.
Bank Logo	Displays the logo of the bank. This field is editable.
Bank Identifier	Displays the external bank identifier. This field is editable.
OAuth Authorization Details	
Enable OAuth Details	Displays the authorization details status for the external bank i.e. whether it is enable /disable. This field is editable.
Authorization URL	Displays the Authorization URL. This field is editable.
Token URL	Displays the Token URL. This field is editable.
Revoke URL	Displays the Revoke url. This field is editable.
Client ID	Displays the Client ID. This field is editable.
Client Secret Keys	Displays the Client keys. This field is editable.
External API Details	

Field Name	Description
External API's	Displays the category of external API's to access data between OBDX and the External Bank. The options are: • Account List • Account Details • Account Summary • Account Activity This field is editable.
API URL	Displays the API URL. This field is editable.

5. Update the required details.
6. Click **Save** to update the changes.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
8. The success message of updates appears.
   Click **OK** to complete the transaction.

43.1.4 Delete External Bank's Details

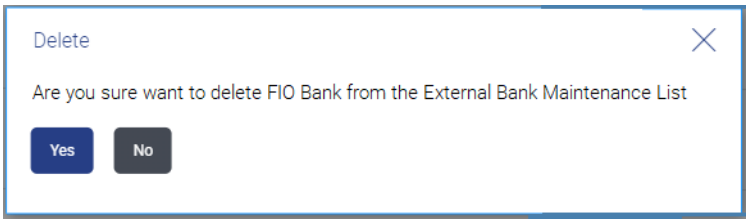
System Administrators can search and delete existing external bank details.

To delete external bank details:

1. In the **Bank Name** field, enter the bank name to search for the specific external bank.
2. Click **Search**.
   List of external banks matching the search criteria appears in search summary section.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
   OR
   Click **Clear** to reset the details.
3. Click **Bank Name** link on **External Bank Maintenance** screen.
   The bank details maintained appears on **External Bank Maintenance - View** screen.
4. Click **Delete** to delete the external bank details.

5. The **Delete Warning** message appears, click **Yes**.

External Bank Maintenance - Delete



6. The **External Bank Maintenance** screen with the successful object deletion message appears. Click **OK** to complete the transaction.

44. Spend Category

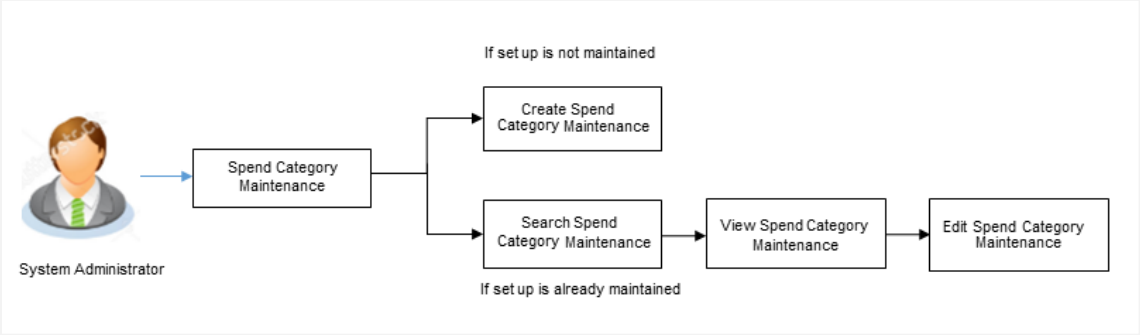
Using this option, the System Administrator can maintain the spend categories. Spend Category maintenance allows the System Administrator to create, modify or expire categories. For each of the Spend Category, System Administrator shall be able to map its corresponding sub categories under which the transactions will be tagged. This maintenance is done only for retail customers. Any time there can be a maximum of 7 categories available and each will have a unique category code. Spend categories cannot be deleted.

The each spend category can have up to four sub categories each.

Prerequisites

- Transaction access is provided to System Administrator
- Transactions which needs to be mapped to different categories are maintained
- Transaction description must have keywords which can be distinguished by rule engine for classification into subcategories

Workflow



Features Supported In Application

The Spend Category maintenance allows the System Administrator to:

- Search and View Spend Category
- Create Spend Category
- Edit Spend Category
- Add Spend Sub Category
- Edit Spend Sub Category

How to reach here:

System/ Bank Administrator Dashboard > Personal Finance > Spend Category
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Personal Financial Management > Spend Category

44.1 Spend Category - Search

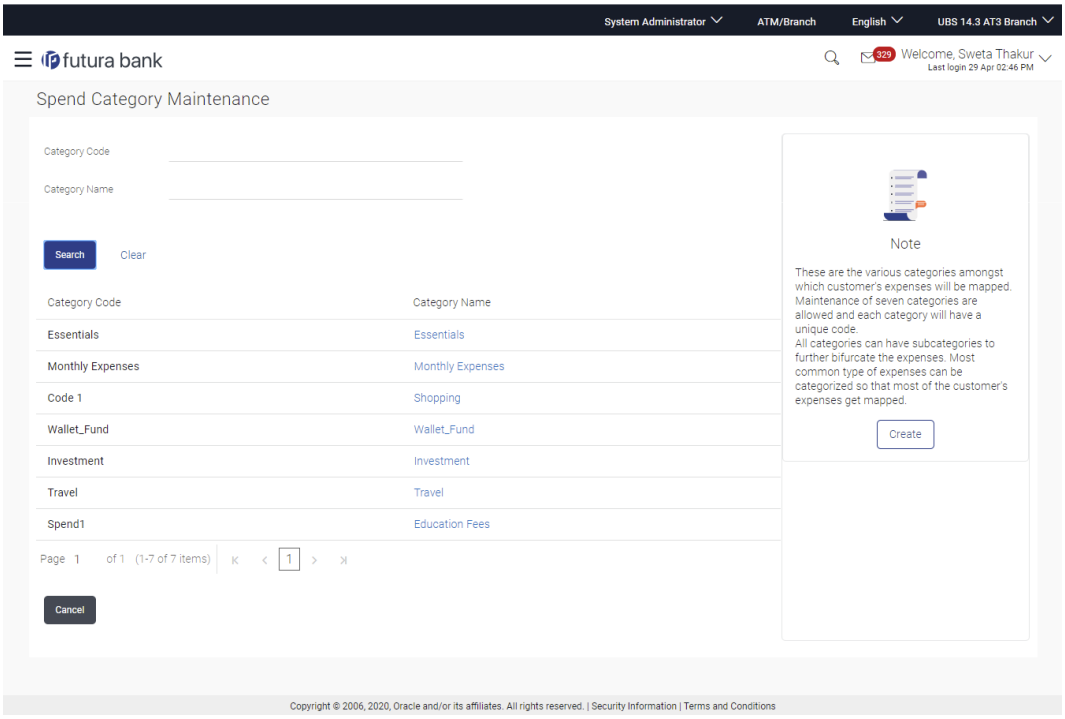
Using Spend category search option, System Administrators search the existing spend category. The search result displays a particular spend categories based on search criteria entered.

If the search parameters are not specified, then it displays all the records.

To search a spend category:

1. Enter the search criteria, click **Search**. The search results appear on the **Spend Category** screen based on the search parameters.
   OR
   Click **Clear** if you want to reset the search parameters.
   OR
   Click **Cancel** if you want to cancel the transaction.

Spend Category - Search



Field Description

Field Name	Description
Category Code	Unique ID maintained for the spend category.

Field Name	Description
Category Name	Name of the spend category. Transactions are mapped to the category name to classify spending under each category.
Search Results	
Category Code	Category codes of the searched spend categories.
Category Name	Name of the searched categories.

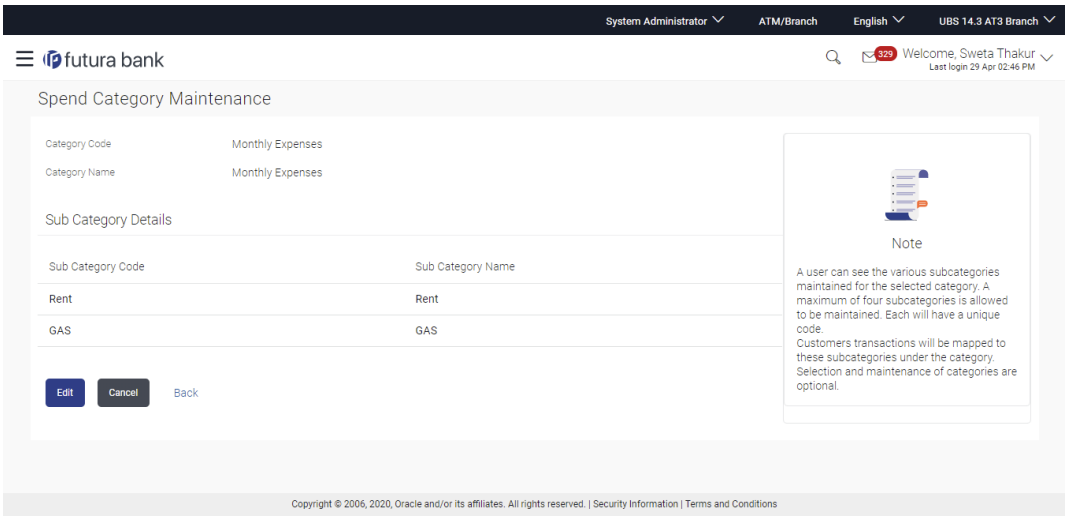
44.1.1 Spend Category - View

Using spend category view option, the System Administrator can view the spend categories and sub categories.

To view a spend category:

1. Enter the search criteria, click **Search**. The search results appear on the **Spend Category** screen based on the search parameters.
2. Click the Category Name link of the record for which you want to view the spend category. The **Spend Category - View** screen appears.

Spend Category - View



Field Description

Field Name	Description
Category Code	Unique ID maintained for the spend category
Category Name	Name of the category. Transactions are mapped to the category name to classify spending under each category.
Sub Category Details	
Sub Category Code	Unique ID maintained for the spend sub-category.
Sub Category Name	Name of the subcategory based on the category name. Transactions can be further classified under the sub categories available under a category. For e.g. Spend category name could be Household Expenses and under that, sub categories could be Grocery, Rent etc.

3. Click **Edit** to if you want to edit the spend category.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

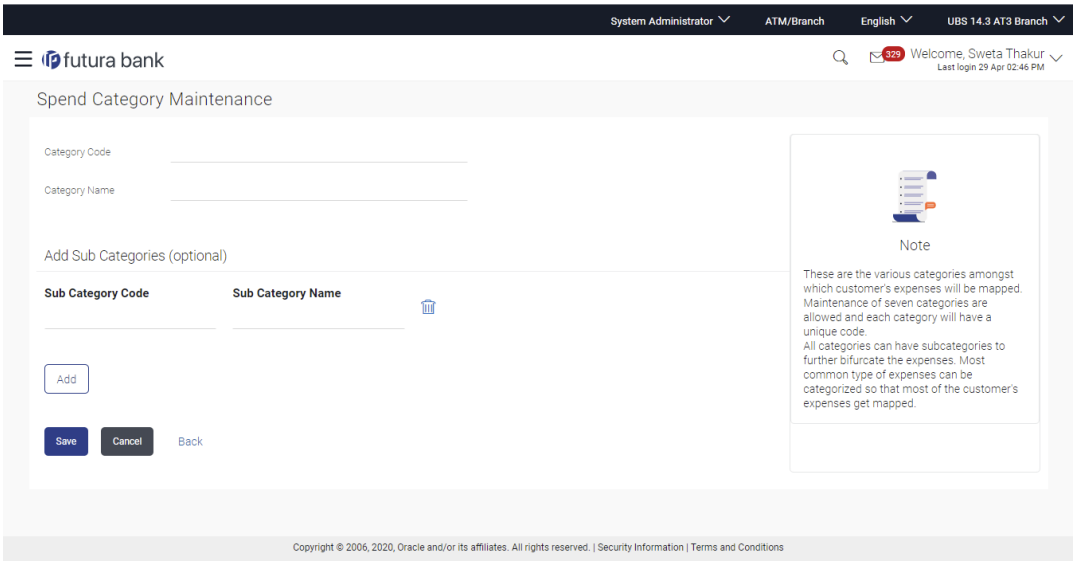
44.2 Spend Category - Create

Using spend category create option, the System Administrator can create new spend categories and sub categories.

To create a spend category:

1. In the **Spend Category** screen, click **Create**. The **Spend Category - Create** screen appears.

Spend Category - Create



Field Description

Field Name	Description
Category Code	Unique ID maintained for the spend category.
Category Name	Name of the category. Transactions are mapped to the category name to classify spending under each category.
Sub Category Details	
Sub Category Code	Unique ID maintained for the spend sub-category.
Sub Category Name	Name of the subcategory based on the category name. Transactions can be further classified under the sub categories available under a category. For e.g. Spend category name could be Household Expenses and under that, sub categories could be Grocery, Rent etc.

2. In the **Category Code** field, enter the code for the spend category.
3. In the **Category Name** field, enter the name of the spend category.
4. In the **Sub Category Details** section, enter the relevant information for subcategories.
5. Repeat step 4 to add more sub categories to a sub category.

Note: You can click to delete a spend sub category or click **Add** to add more spend sub categories.

---

6. Click **Save** to save the category and sub category details.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to modify the details.
   The user will be navigated back to the create screen.
   OR
   Click **Cancel** to cancel the transaction.
8. The success message of spend category creation appears.
   Click **Ok** to complete the transaction.

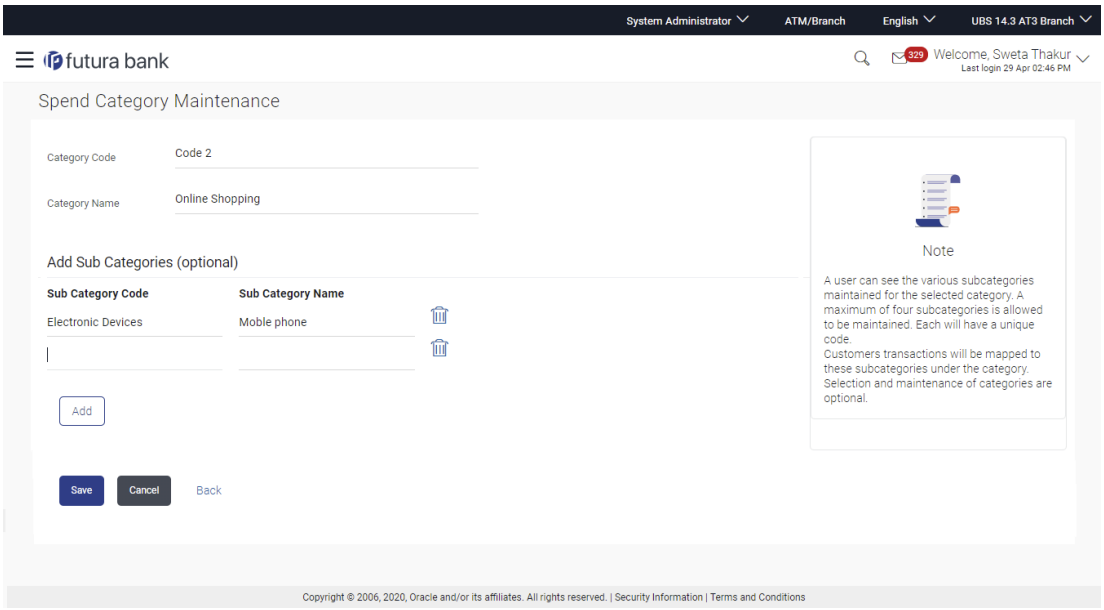
44.3 Spend Category - Edit

Using spend category edit option, System Administrator can modify the spend category details.

To edit or update a spend category:

1. Enter the search criteria, click **Search**. The search results appear on the **Spend Category** screen based on the search parameters.
2. Click the Category Name link of the record for which you want to edit the spend category. The **Spend Category - View** screen appears.
3. Click **Edit** to edit the spend category. The **Spend Category- Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Spend Category - Edit



4. Edit the required details.
5. Click **Save** to update the changes.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to modify the details.
   The user will be navigated back to the create screen.
   OR
   Click **Cancel** to cancel the transaction.
7. The success message of updates appears.
   Click **OK** to complete the transaction.

FAQ

1. How many spend categories can a System Administrator can create?

A System Administrator can create maximum of seven categories. However this is a Data base configuration and can be increased or decreased at the time of implementation.

2. How many spend sub-categories can a System Administrator can create?

A System Administrator can create a maximum of four sub-categories under a main category.

3. What is category code used for?

It is used as a unique key to distinguish different categories.

4. How are the transactions being mapped to the categories?

The categories would be linked to a rule engine which will use some keywords in the description of transaction and get mapped to the category or sub category on its own.

45. Goal Category Maintenance

Goal Category maintenance allows the System Administrator to create, modify or expire goal categories. For each of the Goal Category, System Administrator can map the Product under which the goals will be opened. This maintenance is done only for retail type of parties and is not applicable for corporate type of parties. Any time there can be a maximum of 10 categories available and each will have a unique category code.

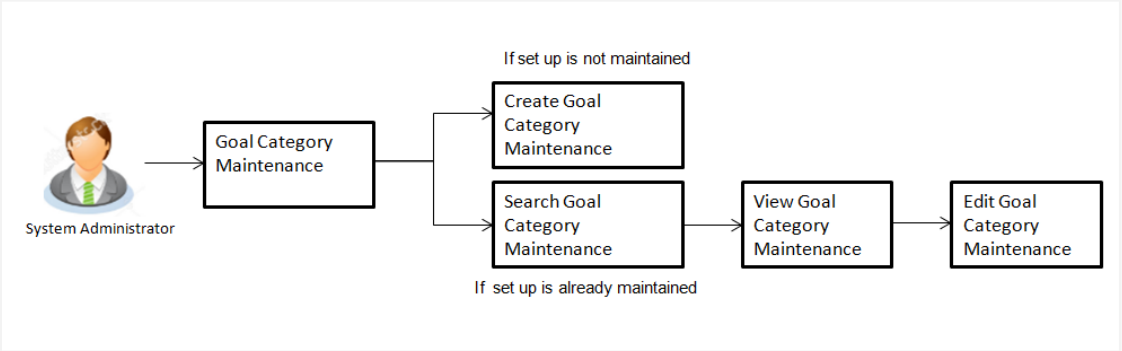
Administrator created categories needs to be linked with a product which will decide the other key parameters which will govern the Goal category. These parameters would be:

- Goal Amount Range (Minimum and Maximum Value)
- Interest Rate Offered
- Tenure Range (Minimum and Maximum)

Prerequisites

- Transaction access is provided to System Administrator
- Products which needs to be mapped to different categories are well maintained
- Goal categories to be made are limited and cannot be deleted

Workflow



Features Supported In Application

Goal category maintenance available for System administrator include

- Search Goal Category
- Create Goal Category
- Edit Goal Category

How to reach here:

System/ Bank Administrator Dashboard > Personal Finance > Goal Category
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Personal Financial Management > Goal Category

45.1 Goal Category - Search

Using this option, System Administrators can search the existing goal category already created. The search result displays matching results of the goal based on search criteria entered.

If the search parameters are not specified, then it displays all the records. The search criteria comprises of two parameters:

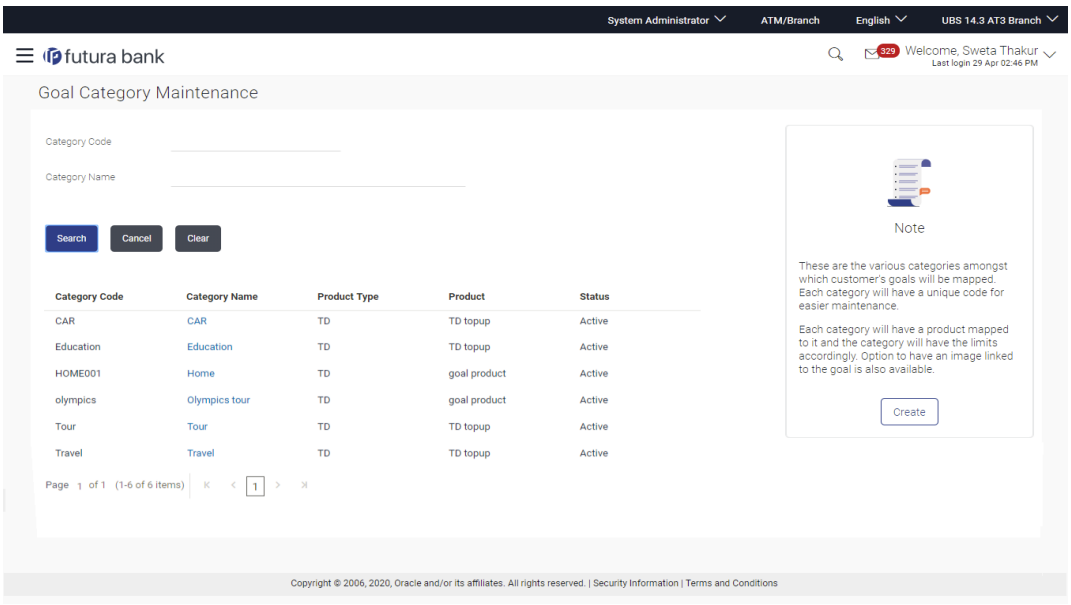
- Category Code
- Category Name

Category code will be a unique code which can be used by administrator to distinguish Goals which can vary on the product mapped.

To search a goal category:

1. Enter the search criteria, click **Search**. The search results appear on the **Goal Category** screen based on the search parameters.
   OR
   Click **Clear** if you want to reset the search parameters.
   OR
   Click **Cancel** if you want to cancel the transaction.

Search Goal Category



Field Description

Field Name	Description
Category Code	Unique ID maintained for the category for internal search for bank administrator.
Category Name	Name of the category.
Search Results	
Category Code	Category code of the searched goal(s).
Category Name	Name of the searched category.
Product Type	Type of product mapped to the category under which the goals are opened.
Product	Name of the product which is mapped to the category.
Status	Status of the category, whether it is active or expired.

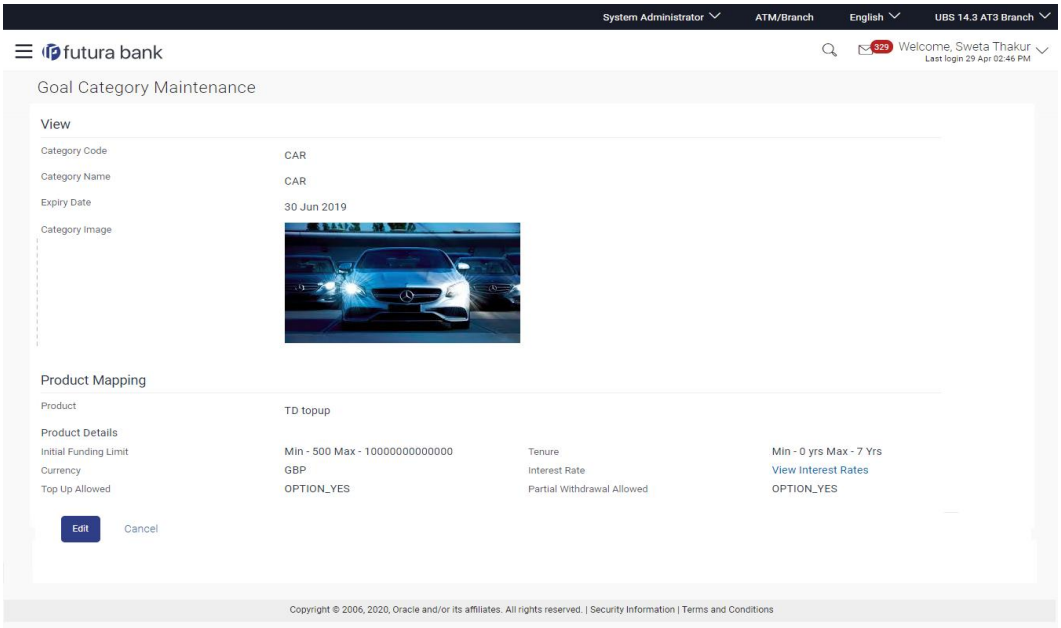
45.1.1 Goal Category - View

Using Goal category view option, the System Administrator can view the goal categories which already exist.

To view a goal category:

1. Enter the search criteria, click **Search**. The search results appear on the **Goal Category** screen based on the search parameters.
2. Click the Category Name link of the record for which you want to view the goal category. The **Goal Category - View** screen appears.

Goal Category - View



Field Description

Field Name	Description
Category Code	Unique ID maintained for the category for internal search for bank administrator.
Category Name	Name of the category.
Expiry Date	Expiry date of the goal category. If the expiry date reaches, the user will not able to view the category.
Category Image	Image assigned for goal category.
Product Mapping	
Product	Name of the product mapped to the category under which the goal shall be opened.
Product Details	
Initial Funding Limit	The initial amount that the user can invest for his goal.
Tenure	The period of the goal created should fall within this range.

Field Name	Description
Currency	The currency with which a goal can be created.
Interest Rate	Click the View Interest Rates hyperlink to view the interest rate slab. Interest rate slab is set for the particular tenure, and is displayed according to the amount selected.
Top Up Allowed	Whether top up for the goal is allowed or not.
Partial Withdrawal Allowed	Whether partial withdrawal of the goal is allowed or not.

3. Click **Edit** to if you want to edit the goal category.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

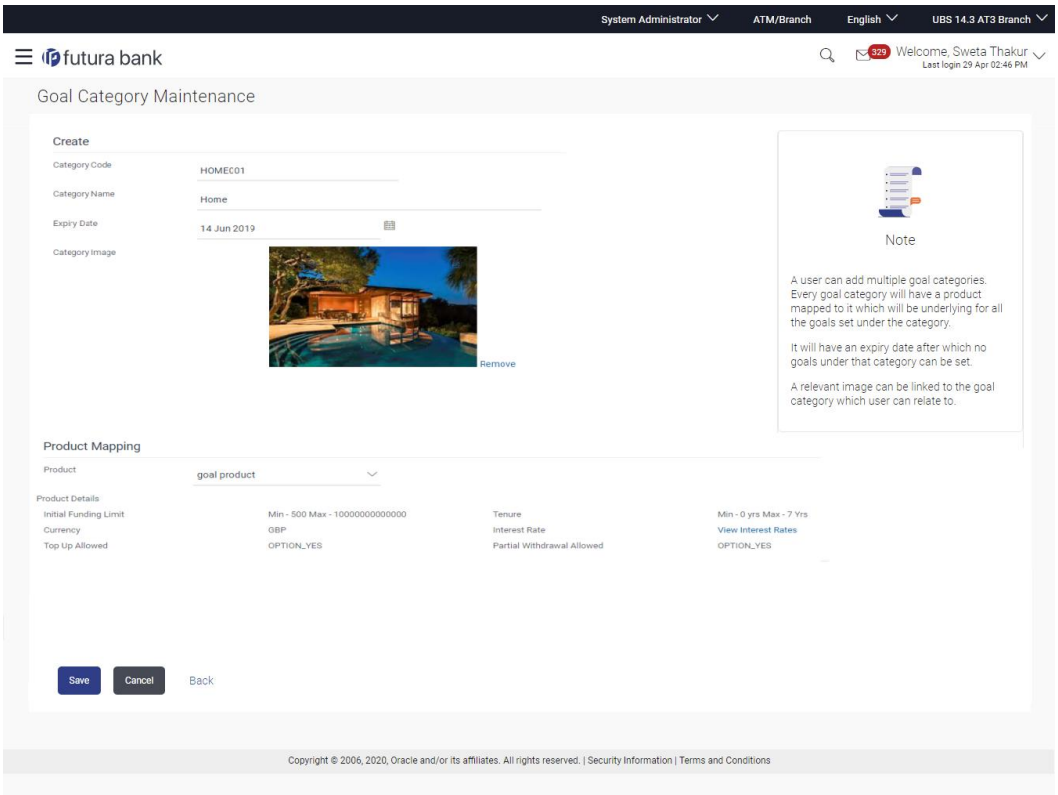
45.2 Goal Category - Create

Using Goal category create option, the System Administrator can create new goal categories and sub categories.

To create a goal category:

1. In the **Goal Category** screen, click **Create**. The **Goal Category - Create** screen appears.

Goal Category - Create



Field Description

Field Name	Description
Category Code	Unique id maintained for the category. Which will be used for internal search for bank administrator.
Category Name	Name of the category.

Field Name	Description
Expiry Date	Expiry date of the goal category. If the expiry date reaches, the user will not be able to view the category while creating a new goal.
Category Image	Image of the category for which category to be created.
Product Mapping	
Product	Name of the product to be mapped to the category under which the goal shall be opened. Bank maintains different products based on the category of the goal.
Product Details	
Initial Funding Limit	The initial amount that the user is investing for his goal. It must be within the limits of the product mapped.
Tenure	The period of the goal created should fall within this range.
Currency	The currency with which a goal can be created.
Interest Rate	Click the View Interest Rates hyperlink to view the interest rate slab. Interest rate slab is set for the particular tenure, and is displayed according to the amount selected.
Top Up Allowed	Whether top up for the goal is allowed or not.
Partial Withdrawal Allowed	Whether partial withdrawal of the goal is allowed or not.

2. In the **Category Code** field, enter the code for the goal category.
3. In the **Category Name** field, enter the name of the goal category.
4. From the **Expiry Date** list, select the appropriate date.
5. Click **Choose Files** to choose the category image.
6. From the **Product** list, select the appropriate option.
7. Click **Save** to save the category details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
8. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.

OR
Click **Back** to navigate to previous screen.

9. The success message of goal category creation appears.
   Click **OK** to complete the transaction.

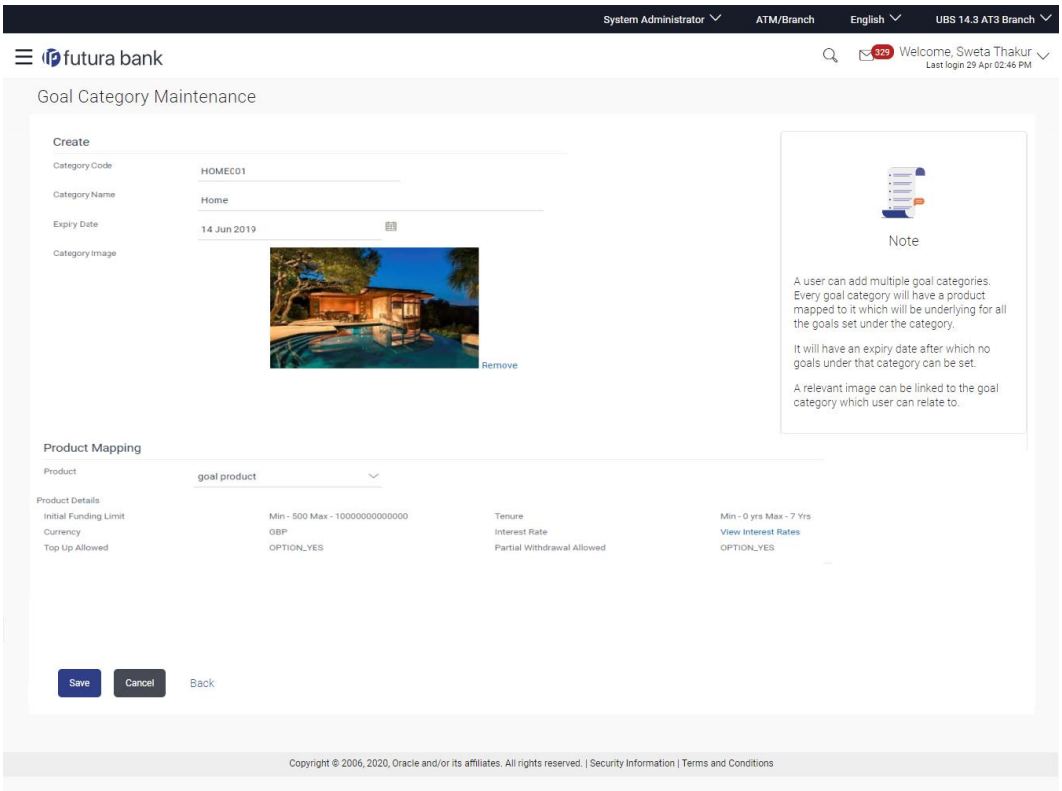
45.3 Goal Category - Edit

Using Goal category edit option, System Administrator can modify the goal details at any time during the tenure of the goal. Administrator can edit Category Name, Expiry Date and Interest Rate fields.

To edit or update a goal category:

1. Enter the search criteria, click **Search**. The search results appear on the **Goal Category** screen based on the search parameters.
2. Click the Category Name link of the record for which you want to edit the goal category. The **Goal Category View** screen appears.
3. Click **Edit** to edit the goal category. The **Goal Category Edit** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

Goal Category - Edit



4. Edit the required details.
5. Click **Save** to update the changes.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
7. The success message of updates appears.
   Click **OK** to complete the transaction.

FAQ

1. Can I create a category with unique category code but a common category name?

No, category code and category name, both should be unique.

2. Can I delete a goal category?

No, goal category once created cannot be deleted. However you can update an expiry date.

3. How many Goal categories can be created?

Administrator can create a maximum of ten goal categories. At a time there can be a maximum of ten active goal categories. Expired goal categories are treated as inactive categories.

46. Experience Builder

Banks can have varied requirements with regards to the theme and for look and feel of the application.

Experience Builder is an administrative maintenance that allows the System Administrator to define the theme using brand logo, colours, fonts and font sizes.

Using the **Manage Columns** feature, bank can configure and enable customizable UI display/download option for the end users. Using this feature, users can personalize the information to be displayed/downloaded from search grid displayed on the screen.

By clicking on '**Manage Columns** option available on the screen, user can

- Rearrange columns
- Remove specific columns.

Note:
1) The downloaded report will have the same columns as displayed on the UI as per user preference as well as there will also be an option to modify the column selection while downloading.
2) The column preferences setup by the user will be saved for future reference i.e. in case the user revisits this screen, the preferred columns will only be displayed in the table.

System Administrator can configure the style / theme by selecting brand logo, header, background, label, button and font colours, font type and sizes for header text, menu, buttons etc. The administrator can define multiple themes with the above-mentioned attributes and once defined, the administrator can activate one of the themes from the available list. The administrator defines brand attributes for user segments.

Pre-requisites

- Transaction access is provided to System Administrator

Features supported in application

- View Experience
- Create Experience
- Edit Experience
- Delete Experience
- Mapping

How to reach here:

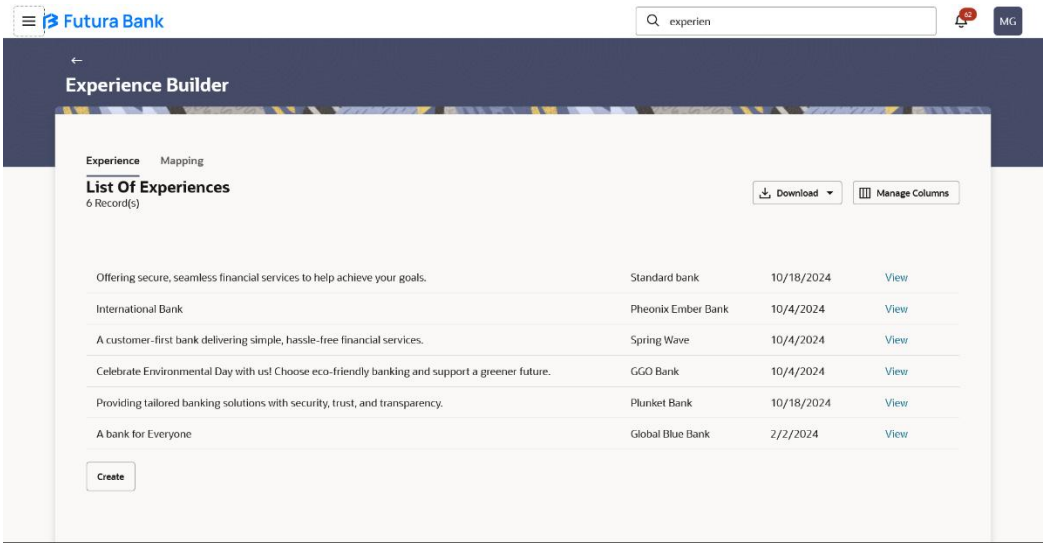
System/ Bank Administrator Dashboard > Toggle menu > Menu > User Experience > Experience Builder
OR
Search > User Experience – Experience Builder

46.1 Experience

Using this option System Administrator can create themes which will be available for Retail user for personalizing his view.

At any point in time, the administrator can deactivate a theme and activate another one.

Experience Builder – Summary



Field Description

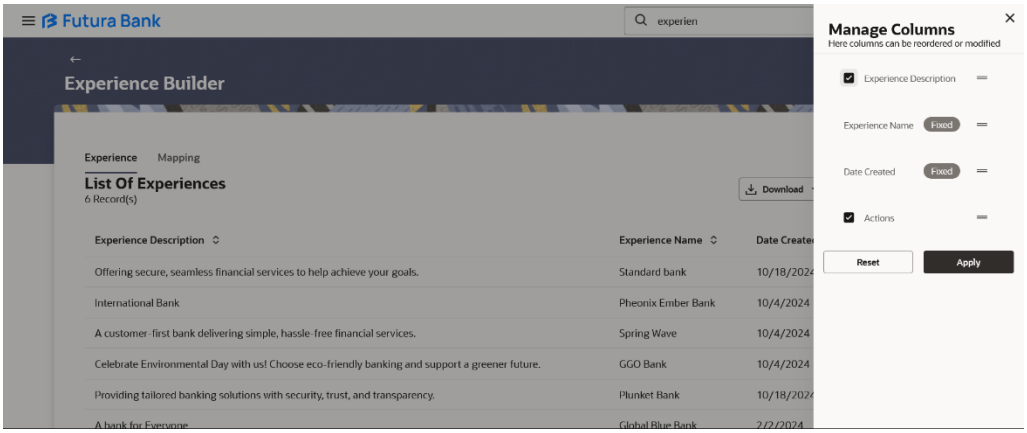
Field Name	Description
Experience Builder Name	Displays the theme name as defined.
Experience Builder Description	Displays the theme description as defined.
Date Created	Displays the date of theme creation.
Actions	The available action buttons against the theme are displayed. The action button can be: • View: Click to view the created theme.

1. Navigate to the **Experience Builder** screen. The application displays the list of experiences.
2. In the **Action** column, click the **View** link to view the already created theme.
   OR
   Click **Create** to create a new theme.

3. Click on the Download to download the records in CSV & PDF format.
   OR

   Click on the Manage Columns to setup a column preferences by rearranging or removing columns.

Experience Builder Summary – Manage Columns



46.1.1 Experience Builder - Create

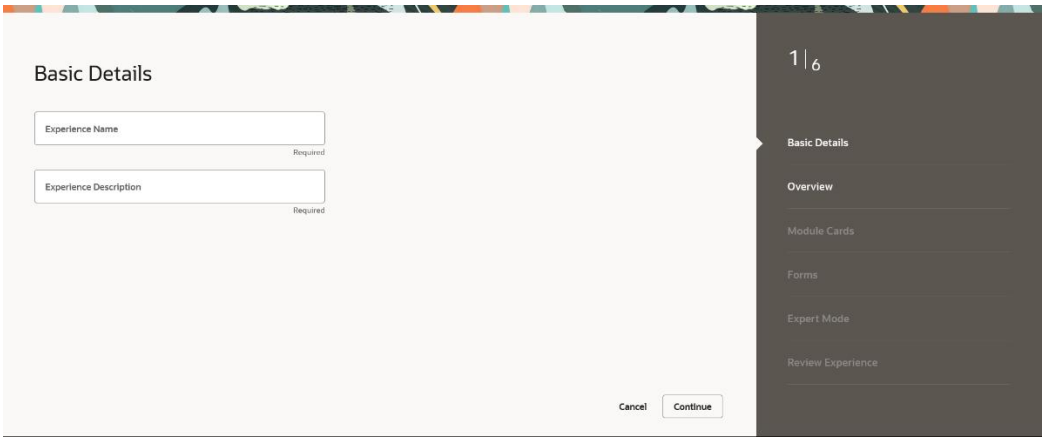
Using this option, System Administrator can create a new theme for retail, corporate and administrator users.

To create a experience:

1. In the **Experience Builder** screen, click **Create**. The screen appears, allowing the user to define the experience in a step-by-step manner..

Note: A preview of how the experience will be displayed, based on the experience definition is appears on the right-hand side of the screen.

Experience Builder – Create -Basic Details - Step 1

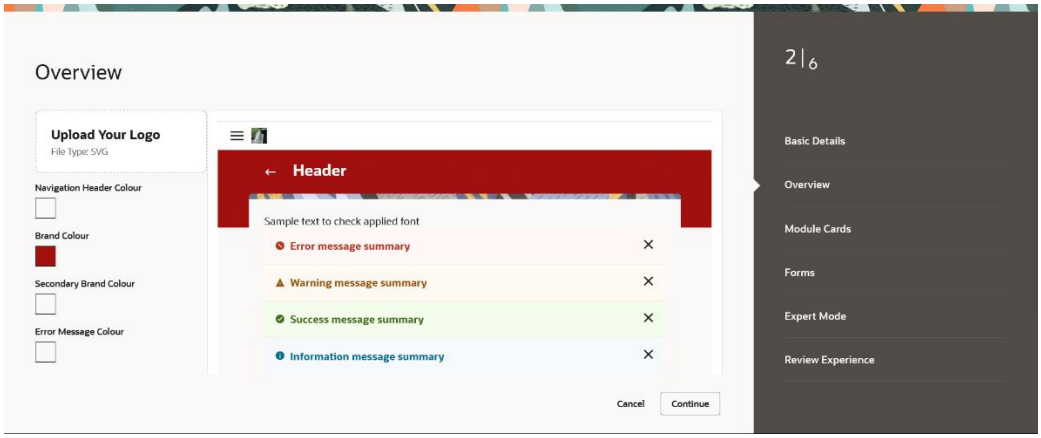


Field Description

Field Name	Description
Experience Name	Enter a name for the experience being created.
Experience Description	Enter a description for the experience being created.

2. Enter the **Basic Details**.
   d. In the **Experience Name** field, enter the name of the theme.
   e. In the **Experience Description** field, enter the description for the theme.
3. Click **Continue** to proceed to the next step.
   OR
   Click **Cancel** to cancel the transaction.

Experience Builder Manage Brand -– Overview -Step 2



Field Description

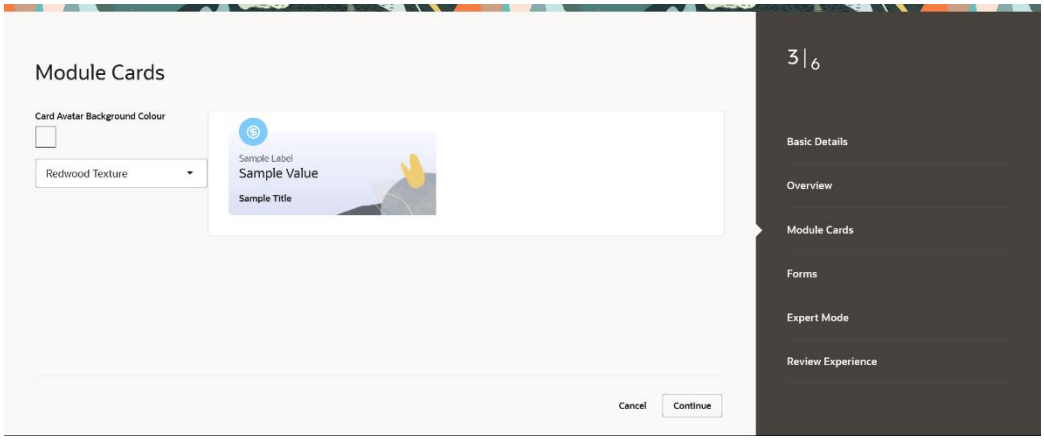
Field Name	Description
Upload Your Logo	Upload a logo file for the experience. **Note**: The allowed format for logo is svg.
Navigation Header Colour	Specify the colour for the navigation header from the colour palette.
Brand Colour	Specify the colour for the brand from the colour palette.
Secondary Brand Colour	Specify the secondary brand colour from the colour palette.
Error Message Colour	Specify the colour for the error message from the colour palette.
Warning Message Colour	Specify the colour for the warning message from the colour palette.
Success Message Colour	Specify the colour for the success message from the colour palette.
Information Message Colour	Specify the colour for the information message from the colour palette.

Field Name	Description
Font Family	The name of the base font family that is to be applied for creating the experience.
Font Family Source (URL)	The URL for the base font that is to be used in the experience.
Page Header Background Colour	Enable or disable the switch to add or remove background colour to page header.
Apply Glass Morphism	Enable or disable the switch to activate or deactivate the glass morphism effect in experience.
Dashboard Tabs	Enable or disable the switch to add or remove dashboard tabs.
Strip Colour	Specify the strip colour you wish to set. The options are: • Default • Brand Colour • Secondary Brand Colour
Main Content Background Colour	Specify the main content background colour you wish to set. The options are: • Default • Brand Colour • Secondary Brand Colour
Body Background Colour	Specify the background colour you wish to set for the body. The options are: • Default • Brand Colour • Secondary Brand Colour
Header Height	The height of the experience header. The options are: • Compact • Wide

Field Name	Description
Header Padding	Specify the space between header content and border. The options are: • Extra Wide • Wide • Vertical Extra Wide • Vertical Wide
Body Strip Colour	Specify whether you wish to show or hide the body strip colour.

4. Set the attributes listed in the **Overview**.
5. Click **Upload Logo** to browse and upload the logo for brand.
6. Select the colours and typography to be assigned to the various components of messages.
7. Define the background colour and font size for various components in the application.
8. Enter the base font family name and base font URL.
9. Click **Continue** to proceed to the next step.
   OR
   Click **Cancel** to cancel the transaction.

Experience Builder Manage Brand – Module Cards -Step 3

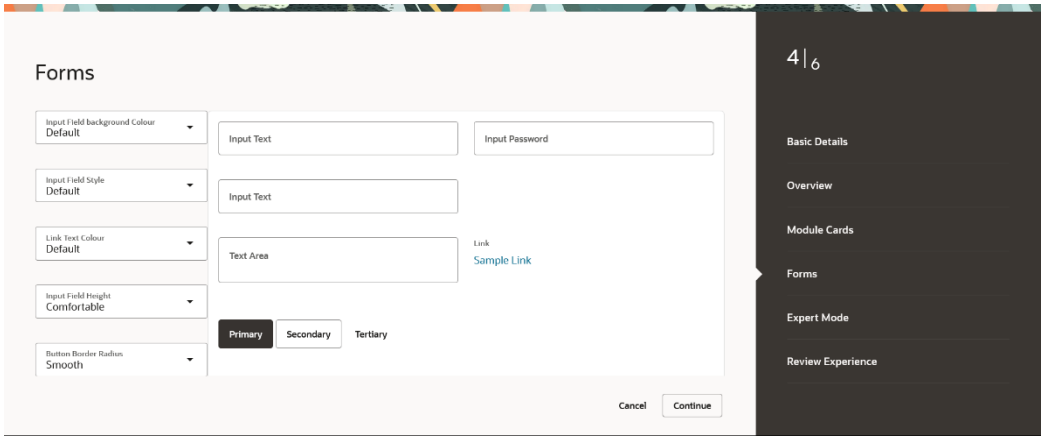


Field Description

Field Name	Description
Card Avatar Background Colour	The card avatar background colour you wish to set.
Card Avatar Background Texture	Specify the background texture for the cards. The options are: • None • Floating Squares • Rotating Squares • Shooting Stars • Redwood Texture

10. Set the attributes of the **Module Cards**.
11. Click **Continue** to proceed to the next step.
    OR
    Click **Cancel** to cancel the transaction.

Experience Builder Manage Brand – Forms -Step 4



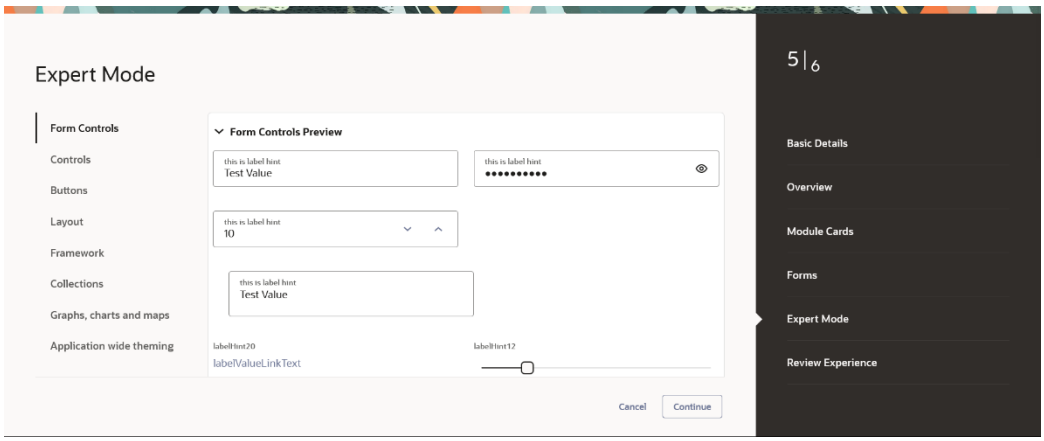
Field Description

Field Name	Description
Input Field Background Colour	Specify the background colour for the input field. The options are: • Default • Brand Colour • Secondary Brand Colour
Input Field Style	Specify the typography weight for the input field. The options are: • Default • Underlined • Circular • Sharp
Link Text Colour	Specify the colour for the link text. The options are: • Default • Brand Colour • Secondary Brand Colour
Input Field Height	Specify the typoghraphy height for the input field. The options are: • Comfortable • Large • Compact
Button Border Radius	Specify the button border style for the button. The options are: • Sharp • Smooth • Rounded • Circular

Field Name	Description
Button Colour	Specify the colour for the button. • Default • Brand Colour • Secondary Brand Colour
Label Position	Specify the label position. The options are: • Top • Inside • Start
Direction	Specify the page layout direction. The optios are: • Row • Column
Maximum Columns	Specify the maximum columns permitted in the page layout. The options are: • One • Two • Three

12. Set the attributes of the **Forms**.
13. In the **Form**s section, select the form background colour and typography for form header, form disabled input, label, info text icon and links.
14. Click **Continue** to proceed to the next step.
    OR
    Click **Cancel** to cancel the transaction.

Experience Builder Manage Brand – Expert Mode -Step 5



Field Description

Field Name	Description
Form Controls	A structural representation of user related input fields is known as a form for example Input Text, Drop-Down list, Links, Password Label, Slider, Switch Buttons, Toggle Buttons, Checkboxes etc. The application form related attributes are defined in this section. The Forms related variables are listed here, which are editable. A preview of how the form will be displayed, based on brand definition is focused and appears on the right-hand side of the screen.
Controls	Displays the variables for the controls like Headings, Links, Menu buttons, Action list, Navigation. This is editable. The typography colour, font size and weight are defined here. Headings- The header text Link Text Menu button- Actions with a single tap Navigation- Element that appears as quick links which makes switching between different pages of the same component.
Buttons	An element that allows the user to take actions with a single tap and interact with them is known as the button. The application buttons like Toggle buttons, Switch buttons related attributes are defined in this section. The Buttons related variables are listed here, which are editable. A preview of how the buttons will be displayed, based on brand definition is focused and appears on the right-hand side of the screen.

Field Name	Description
Layout	The layout section comprises of the various layout components available throughout the application, such as Navigation List, Tab Bar, Panel, and Dialog. This section also provides control over the current Masonry Layout in the application.
Framework	The framework preview shows the user, all the possible font hierarchies in the system, along with badges for different types of messages in the applications.
Collections	The collections preview displays the various types of collection components available in the application, such as List View and Table. Note: The collections components can be referred from the Oracle Jet Library.
Graphs, Charts and Maps	The different types of visualizations available in the application such as rating gauge, charts are defined and can be modified in this section. Note: The visualization components can be referred from the Oracle Jet Library.
Application wide theming	This section consists mainly of the different variables available to be edited by the admin which will affect application wide classes, such as colour palettes, scrollbar properties and more.

15. Set the attributes listed under the **Expert Mode**.
    a. In the **Menu** section, select the background, typography, menu hover colour and interaction type for the menu to be defined.
    b. In the **Table** section, select the background, typography of table header and table body.
    c. In the **Form** section, select the form background colour and typography for form header, form disabled input, label, info text icon and links.
    d. In the **Button/ Button Sets** section, select the values for border, background and typography for primary, secondary, tertiary, help button and other buttons.
    e. In the **Generic Components** section, define the background colour and font size for various components in the application.
    f. In the **Modal Window** section, select the values for modal window header, and modal window body.
    g. In the **Navigation Bar** section, colours to be assigned to the various components that form part of the navigation bar.
    h. In the **Confirmation/ Error Banner** section, select the colours and dimension to be assigned to the various components that form part of confirm/error banner.

i. In the **Scroll Bar** section, click and select the border colours for scroll track and scroll thumb.

j. In the **Accordion** section, select the colours and typography to be assigned to the various components of accordion.

k. In the **Overlay** section, select the background colours and header typography to be assigned to the various components of overlay window.

l. In the **Message** section, select the colours and typography to be assigned to the various components of alert messages.

16. An example of how the various components of the brand will be displayed, based on brand definition appears in the form section (right hand side) of the screen.

17. Click **Continue** to proceed to the next step.
OR
Click **Cancel** to cancel the transaction.

18. The **Review** screen appears. Verify the details.

Note: Click the ● ○ ○ (paging control)icon to navigate between pages.

Click **Save** to save the details.
OR
Click **Cancel** to cancel the transaction.

19. The success message appears along with the status of maintenance. Click **OK** to return to the dashboard.

46.1.2 Experience Builder - View

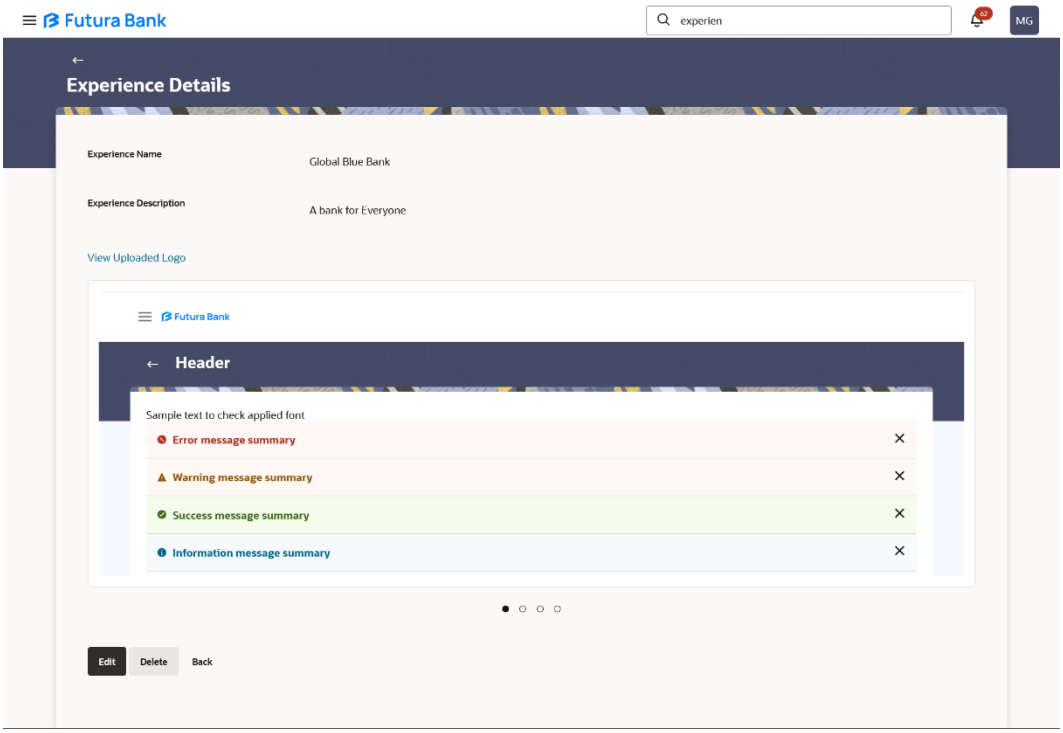
Using this option System Administrator can view the created theme or brand.

To view the experience:

1. Navigate to the **Experience Builder** screen. The application displays the list of experiences.
2. In the **Action** column, click **View** against the brand which you want to view. The **Experience Builder - View** screen appears.

Note: Click the ● ○ ○ icon to navigate between pages.

Experience Builder - View



3. Click on the **View Uploaded Logo** link to view the brand logo.
   OR
   Click **Edit** to edit the theme. The **Experience Builder - Edit** screen appears.
   OR
   Click **Delete** to delete the experience.
   OR
   Click **Back** to navigate to the previous screen.

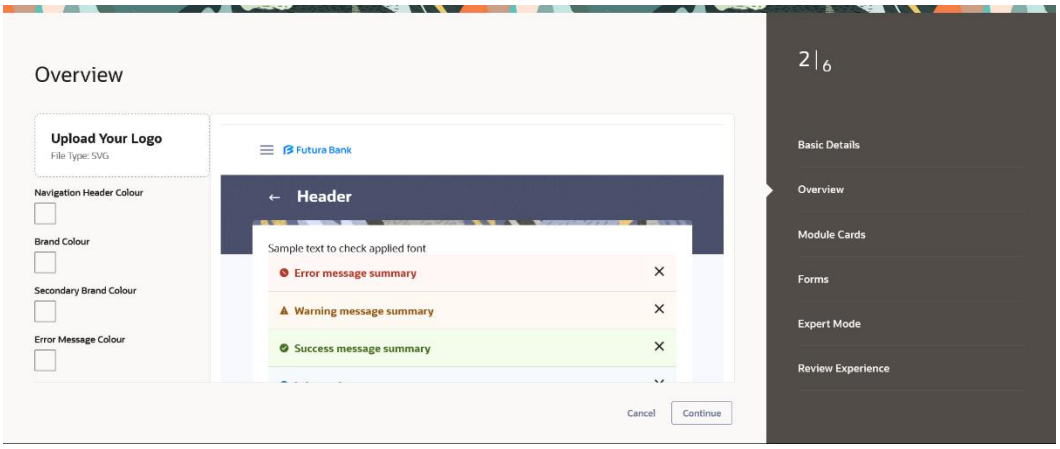
46.1.3 Experience Builder - Edit

If the defined theme does not suit the requirement, then system administrator can edit the defined experience using the Edit option.

To edit the experience:

1. Navigate to the **Experience Builder** screen. The application displays the list of experiences.
2. In the **Action** column, click **View** against the brand which you want to view. The **Experience Builder - View** screen appears.
3. Click **Edit** to edit the experience. The **Experience Builder** screen appears in editable mode.
   OR
   Click **Delete** to delete the experience.
   OR
   Click **Back** to navigate to the previous screen

Experience Builder - Edit



For more information on the fields refer **Field Description : Experience Builder – Create**.

4. Edit the required attributes.
5. Click **Update** to save the changes.
   OR
   Click **Cancel** to cancel the transaction..
6. The **Review** screen appears. Verify the details.
   Click **Save** to save the details.
   OR
   Click **Cancel** to cancel the transaction.
7. The success message appears along with the status of maintenance. Click **OK** to return to the dashboard.

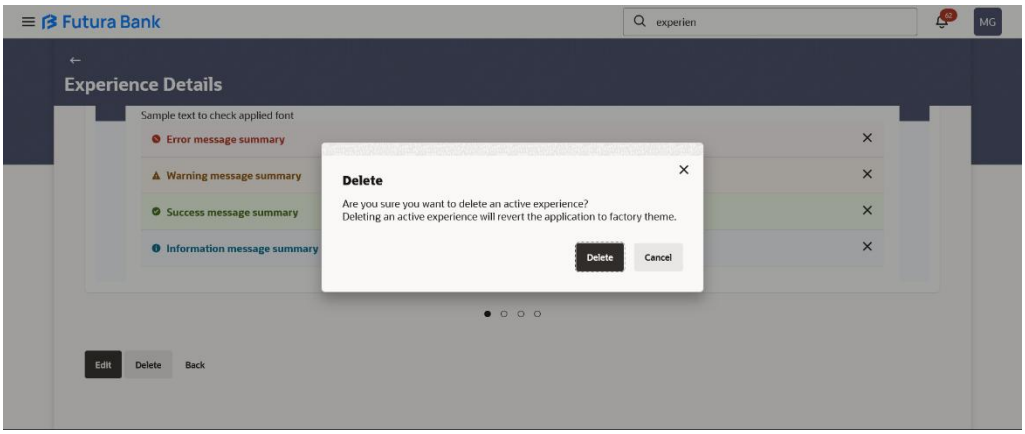
46.1.4 Experience Builder - Delete

The System Administrator can delete a created experience maintained in the application.

To delete the experience:

1. Navigate to the **Experience Builder** screen. The application displays the list of experiences.
2. In the **Action** column, click **View** against the brand which you want to view. The **Experience Builder - View** screen appears.
3. Click **Delete**. A message appears asking the user to confirm brand deletion. Click **Delete** to confirm deletion of the experience.
   OR
   Click **Cancel** to cancel deletion and return to the **Experience Builder – View** screen.

Delete Experience Builder



4. The success message appears along with the status of the maintenance. Click **OK** to return to the dashboard.

46.2 Mapping

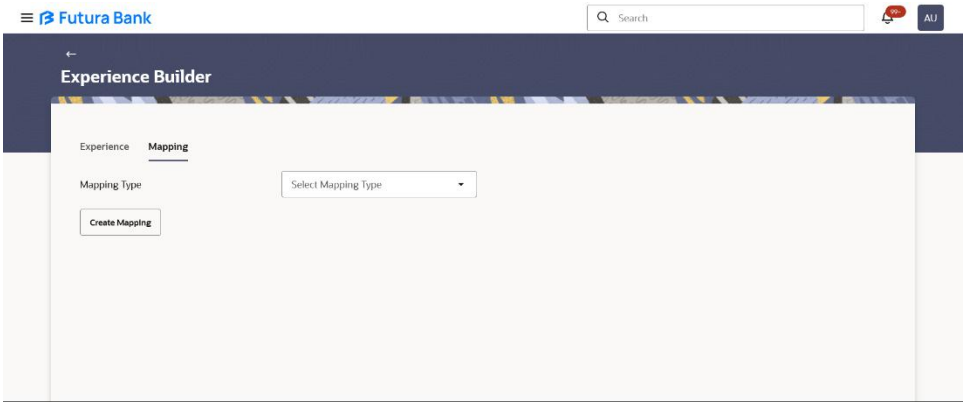
Using this option System Administrator can map the existing brands to any user, party, role or entity.

46.2.1 Experience Mapping Search

To view the brand mapping details:

1. In the **Experience Builder** screen, click the **Mapping** tab. The **Experience Builder - Mapping** screen appears.

Mapping

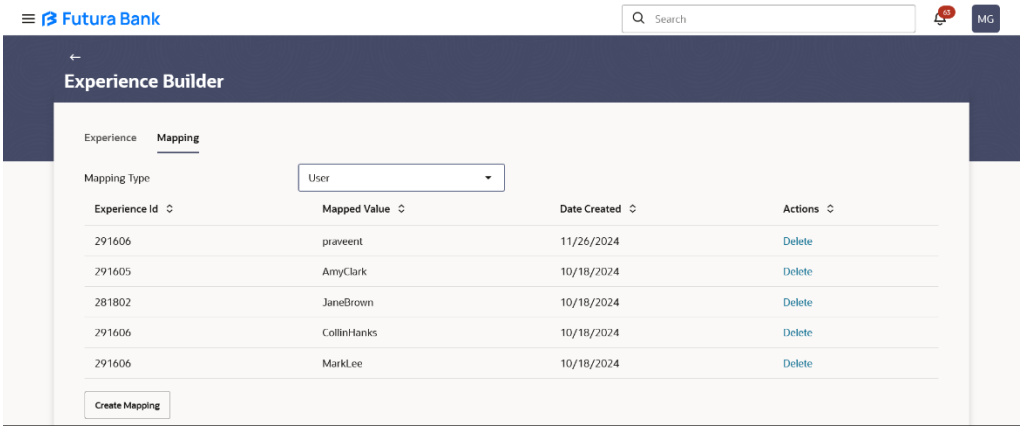


Field Description

Field Name	Description
Mapping Type	A list of options for the mapping type to search which brand it is mapped to appear. The options are: • User • Party • Segment • User Type • Entity

2. From the **Mapping Type** list, select the option for which you want to view the mapping. The **Experience Builder – Search Results** appear.

Experience Builder - Experience Mapping Summary



Field Description

Field Name	Description
Experience Mapping Summary	
Experience Builder **Id**	The identification number of the mapped theme.
Mapped Value	The value, which is mapped to the experience. The mapped value depends on the selected mapping type. For example, If the mapping type is 'user' the mapping value will be 'user ID', If the mapping type is 'party' the mapping value will be 'party ID', If the mapping type is 'role' the mapping value will be user role, such as 'Corporate' 'Retail' and 'Administrator', If the mapping type is 'entity' the mapping value will be 'entities'.
Mapping Type	The level at which the experience is mapped.
Date Created	The date on which the experience mapping was performed.
Actions	The available actions that can be performed against the experience mapping are displayed. The options can be: • Delete

3. Click **Delete** against a record to delete the brand mapping.
   OR
   Click **Create Mapping in the Help Panel,** to create a experience mapping.

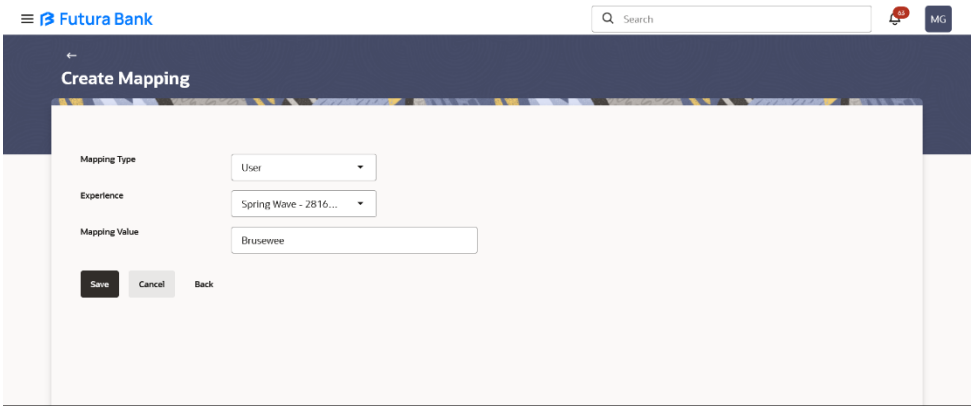
46.2.2 Create Mapping

Using this option System Administrator can create a experience mapping.

To create the experience mapping:

1. In the **Mapping** tab, click **Create Mapping** .. The **Experience Builder - Create Mapping** screen appears.

Experience Builder - Create Mapping



Field Description

Field Name	Description
Mapping Type	Select the level at which the experience is to be mapped. The options are: • User • Party • User Type • Entity
Experience	Select a experience to be mapped at the level selected under Mapping Type.
Mapping Value	Enter a mapping value. This field appears if you select **Party** option from the **Mapping Type** list, click the **Party Search** link and search for a party. The result will populate in the **Mapping Value** field.
Segment	Segment of the user for which the value is to be mapped. This field appears if you select **User Type** option from the **Mapping Type** list.

2. From the **Mapping Type** list, select the appropriate option to be mapped.
3. From the **Brand** list, select a experience.
4. In the **Mapping Value** field, enter the value to be mapped.
   OR
   If you have selected **Party** option from the **Mapping Type** list, click **Party Search**, to search the party Id. The Mapping Value field gets populated.
   If you have selected User Type option from the Mapping Type list, click **Segment** list to select the segment.
5. Click **Save**.
   OR
   Click **Cancel** to cancel the maintenance.
   OR
   Click **Back** to return to the previous screen.
6. The success message along with the status of maintenance appears. Click **OK** to return to the dashboard.

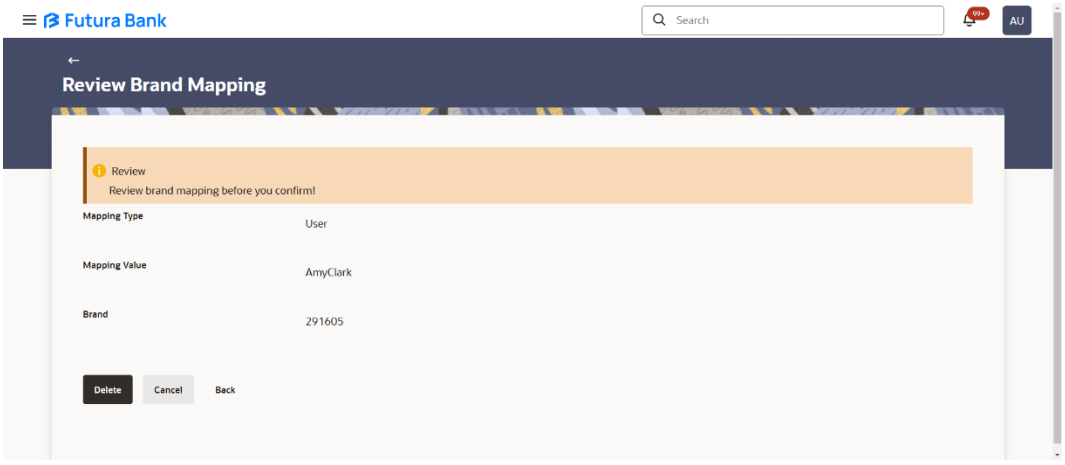
46.2.3 Delete Mapping

Using this option System Administrator can delete a experience mapping.

To delete a experience mapping:

1. In the **Mapping** tab, select the appropriate option from the **Mapping Type** list. The **Experience Mapping Summary** screen appears.
2. Click **Delete** against a mapping record in the action column, that you want to delete.
3. The **Review** screen appears. Verify the details, and click **Delete**.
   OR
   Click **Back** to return to the previous screen.
   OR
   Click **Cancel** to cancel the maintenance.

Delete Mapping



4. The success message appears along with the status of maintenance. Click **OK** to return to the dashboard.

47. Dashboard Overview

Dashboard Builder provides an ability to the Bank to build custom dashboards.

Dashboard Builder is an administrative maintenance that allows the System Administrator to create and configure dashboard templates for Retail & Business, Corporate and Administrator users.

For the Retail & Business type of user, the Bank administrator can map brands and dashboards at the Party Type level. Thus while accessing Retail Party and Business Party details, the user will be able to see relevant dashboards and brands.

The administrator can further assign the Dashboards at the party level (Retail or Business)/user level, however only the transactions and widgets mapped at the party level will be accessible by the user post login.

System Administrator can configure new dashboards by dragging and dropping the desired widget at desired location in template. System administrator can define the dashboard for a user segment, application role, module and for a user type. Facility is provided to search, view, edit and delete the configured dashboards.

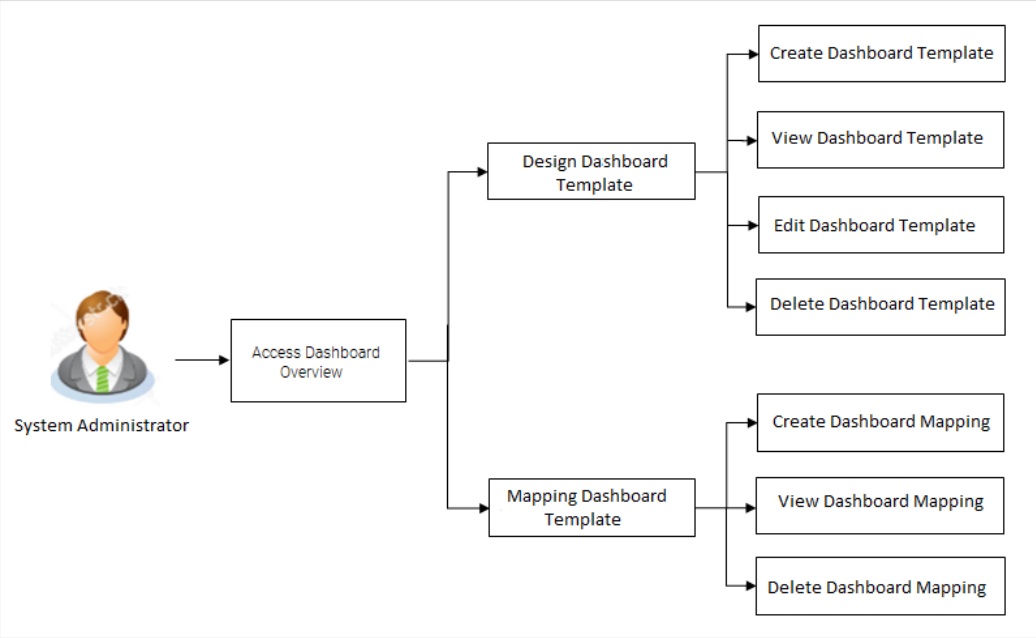
These dashboards are responsive and can adapt to any type of device i.e. desktop, mobile and tablet. System allows the user to design new template and preview it for different types of devices before enabling it. The user can also change the size of the widget (expand and compress) and can remove the widget from the template if desired. The widgets on the dashboard auto adjust itself according to the place available on the dashboard.

The administrator can define multiple dashboards with the various attributes/ widgets. Further these templates can be mapped to the roles, party or even to a specific user.

Prerequisites

- Transaction access is provided to System Administrator
- Approval rule set up for System Administrator to perform the actions
- Application roles are maintained in application and widgets are mapped to application roles

Workflow


Create Dashboard Template
View Dashboard Template
Design Dashboard Template
Edit Dashboard Template
Delete Dashboard Template
Access Dashboard Overview
System Administrator
Create Dashboard Mapping
Mapping Dashboard Template
View Dashboard Mapping
Delete Dashboard Mapping

Features supported in application

Design

- Create New Dashboard
- View Dashboard
- Edit Dashboard
- Delete Dashboard

Mapping

- View Dashboard Mapping
- Create Dashboard Mapping
- Delete Dashboard Mapping

How to reach here:

Bank Administrator Dashboard > Toggle Menu > Menu > User Experience > Dashboard Overview

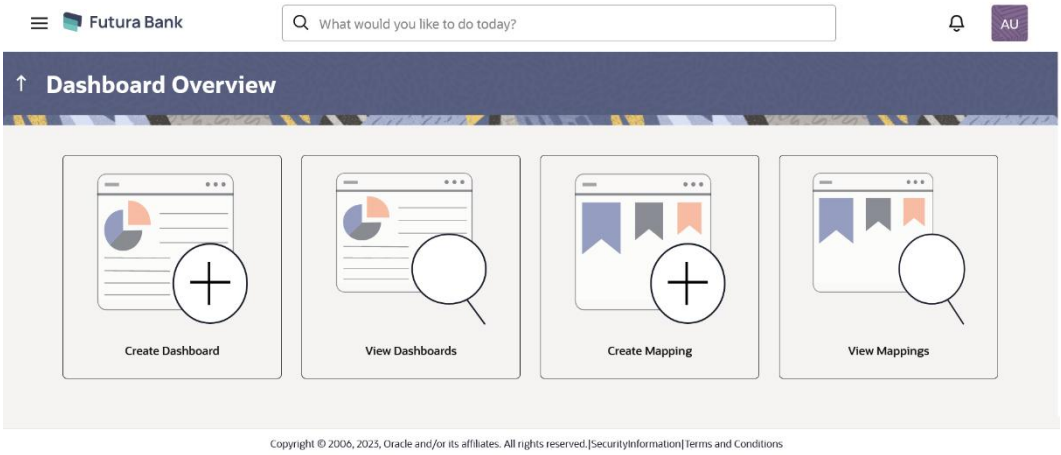
47.1 Dashboard Overview– Summary

Dashboard Overview- Design summary page displays the list of already designed templates, with template name, description, dashboard type, value and date of creation. The administrator can view the dashboard template details by clicking the **View/Edit Dashboard** link in ⋮ menu icon under the **Action** column against the respective template.

To view the Dashboard summary:

1. Navigate to the screen, the **Dashboard Overview** screen appears.

Dashboard Overview



Field Description

Field Name	Description
Create Dashboard	Click to create Dashboard for the specific user segment or module or user type.
View Dashboard	Click to view already created dashboard template.
Create Mapping	Click to create dashboard of the dashboard type, the dashboard template and to a user/party/user segment/user type.
View Mapping	Click to view dashboard mapping already created for the dashboard template with the user/party/user segment/user type.

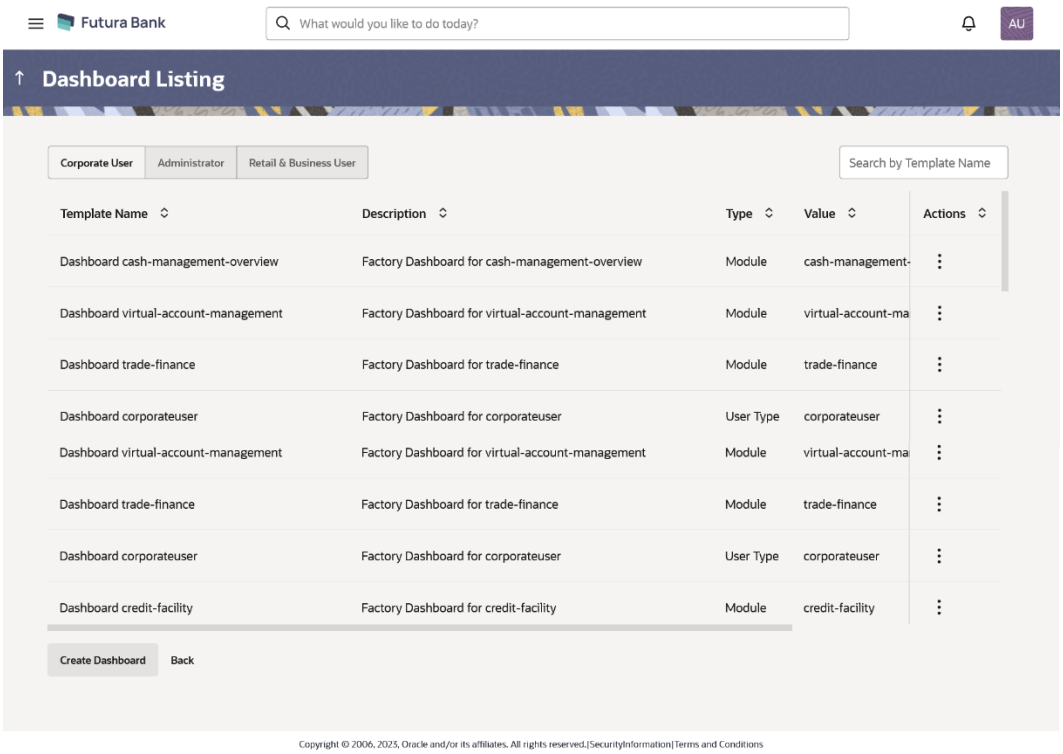
47.2 Dashboard Overview– View

Using this option, System Administrator can view the details of already created dashboard template. The system administrator can view the template in desktop, tablet and for mobile mode by clicking the respective icons.

To search and view a dashboard template:

1. On the **Dashboard Overview** screen, click on **View Dashboard** tab.
   The **Dashboard Listing** screen appears.

Dashboard Overview – Dashboard Listing



Field Description

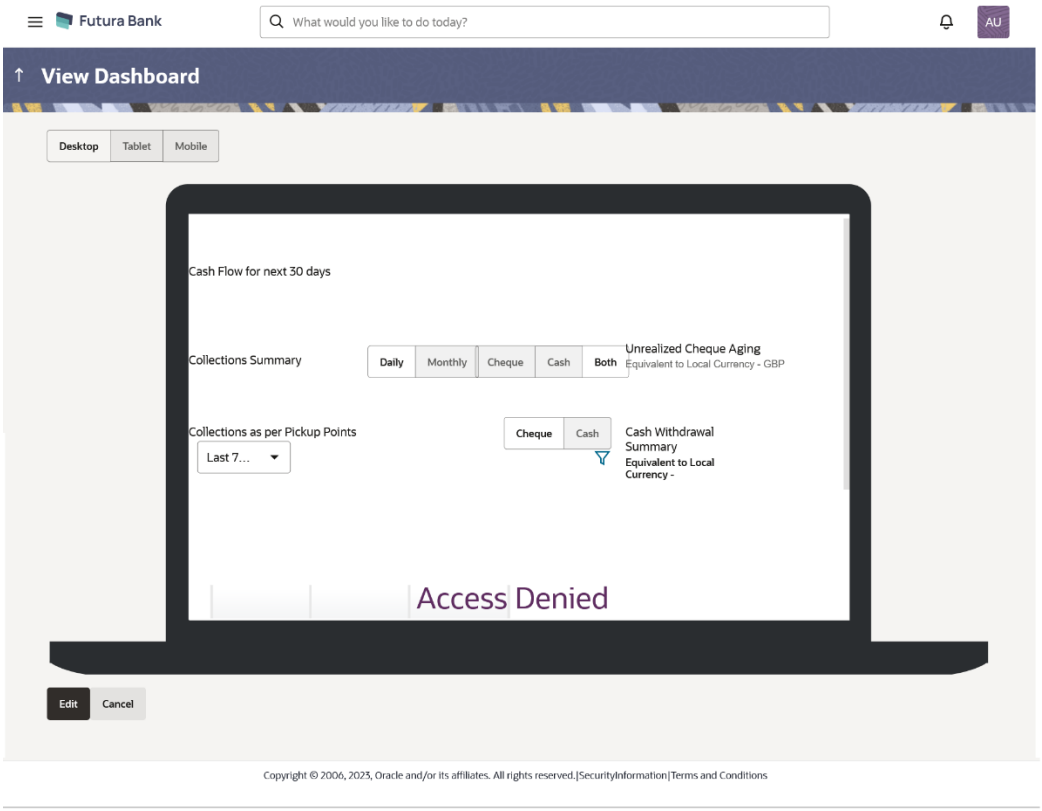
Field Name	Description
User Type	The user type for which the dashboard template needs to be viewed. The options are: • Corporate User • Administrator • Retail & Business User
Template Name	Name of the template that the administrator can enter to view the specific template.
Search Results	
Template Name	Displays the name of the custom dashboard template.
Description	Displays the description as defined for the custom dashboard template.
Type	Displays the type for which the dashboard template is created i.e. segment, user type or module.

Field Name	Description
Value	Displays the name of the segment / module for which the dashboard template is defined.
Actions	The available action buttons against the dashboard template are displayed. The action button can be: • View/Edit Dashboard: Click to view/edit the created dashboard template. • Clone Dashboard: Click to clone an existing dashboard template. • Delete Dashboard: Click to delete existing dashboard template. • Create Mapping: Click to create dashboard mapping of the dashboard type, the dashboard template to a user/party/user segment/user type.

2. In the **Dashboard Listing** screen, select the appropriate type of user in the **User Type** field. All the dashboard templates of the selected user type appears on the screen.
   OR
   In the **Template Name** field, enter the name of the template that you want to search. The searched dashboard template appears on the screen.

3. In **Action** column against the already created dashboard template, click on the icon, and then click **View/Edit Dashboard** link to view the dashboard template details.
   The **Dashboard Overview - View Dashboard** screen appears.
   OR
   Click **Create Dashboard** to create a new dashboard template.
   OR
   Click **Back** to navigate to the previous screen.

View Dashboard Template



4. Click **Edit** to modify the template. The **Dashboard Listing – Edit Dashboard** screen appears.
   OR
   Click **Cancel** to cancel the transaction and navigate to the 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click the **Desktop**/ **Tab**/ **Mobile** icon to view the template in desktop, tab or mobile mode.

47.3 Dashboard Overview – Create

System Administrator can create new custom dashboard template for Retail & Business, Corporate and Administrator user using this option.

As part of creation of custom dashboard, the administrator needs to select the appropriate tab for which the dashboard needs to be created/ designed i.e. user segment or module or user type.

System will facilitate the user with a default dashboard available and the administrator can decide to create a custom dashboard by dragging and dropping new widgets available from the list of widgets.

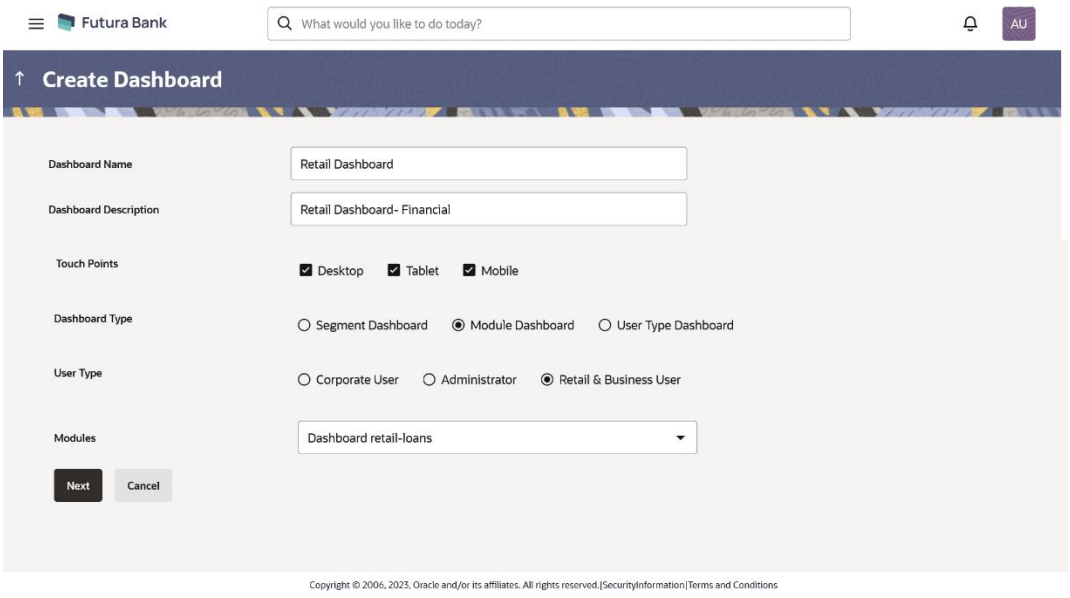
Following types of dashboard can be created:

- Segment Dashboard - Design dashboard for a user segment
- Module Dashboard - Design dashboard for the available application modules i.e. CASA, Term Deposit, Loans etc.
- User Type Dashboard - Design dashboard for a user type i.e. Retail & Business, Corporate or Administrator.

To create a new dashboard template:

1. On the **Dashboard Overview** screen, click on **Create Dashboard** tab.
   The **Create Dashboard** screen appears.

Create Dashboard Template



Field Description

Field Name	Description
Template Name	Name of the template that the System Administrator user wants to create.
Template Description	Description for the template.
Design	The type of device on which the template will be enabled.
Select Module	System lists the dashboard for the segments / user type / module depending on the option selected.

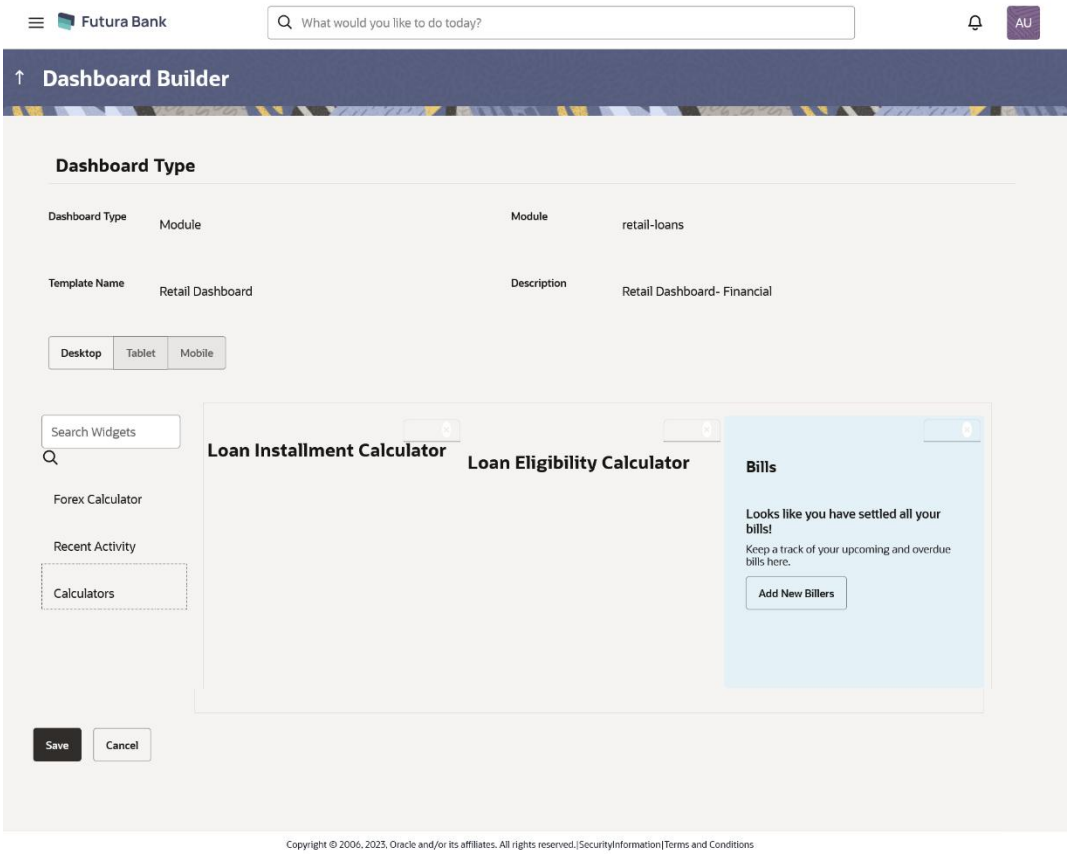
Field Name	Description
User Type	Select the user type for which the dashboard needs to be created. Note: If dashboard needs to be created for a user segment then user type 'Retail & Business' needs to be selected. User Segment is not supported for Corporate and Administrator user.
Select Module Icon	Select the dashboard icon that is displayed based on the selected segments / user type / module.
List of Dashboards	System displays the list of dashboards available for selection based on the selected module type.

2. In the **Template Name** field, enter the name of the new template that is to be created.
3. In the **Template Description** field, enter the description of the new template.
4. To enable the template for Desktop/ Tablet / Mobile, select the required options from the **Design** check box.
5. From the **Segment Dashboard / Module Dashboard/ User Type Dashboard** tabs, select the appropriate module. The **Dashboard Overview - Design** screen of the selected module appears.
   For example, Retail & Business is selected from the **User Type Dashboard**. The **Dashboard Overview** - **Design template** for retail & business user appears.
6. In the **User Type** field, select the appropriate user type.

Note: If dashboard needs to be created for a user segment then user type 'Retail & Business' needs to be selected. User Segment is not supported for Corporate and Administrator user.

7. Select the appropriate dashboard from the list of dashboards displayed based on the selected module.
8. Click **Next**. The **Create Dashboard** template screen appears.
   OR
   Click **Cancel** to cancel the transaction and navigate to the 'Dashboard'.

Create Dashboard Template



9. Click on the desired widgets from the widget list to appear on dashboard.
   OR
   In the **Search Widget** field, enter the name of the widget that you want to appear on the dashboard and click .icon.
   OR
   Click on the desired widgets of the dashboard to the desired location. System highlights the area where the widget can be placed.
10. Click on the upper right corner of the widget, if you want to expand the widget.
    OR
    Click on the upper right corner of the widget, if you want to compress the widget.
    OR
    Click on the upper right corner of the widget, if you want to remove the widget from the dashboard.
11. If the selected widget has multiple widgets on the same like quick links, select the required widget that you want to appear on the dashboard.
12. Click **Save** to save the template.
    OR
    Click **Cancel** to cancel the transaction and navigate to the 'Dashboard'.
    OR
    Click **Back** to navigate to previous screen.

13. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click the **Desktop**/ **Tab**/ **Mobile** icon to review the created template in desktop, tab or mobile mode.
    OR
    Click **Cancel** to cancel the transaction.
    A warning message of cancelling the operation appears. Click **Yes** to confirm.
    OR
    Click **Back** to navigate to previous screen.
14. The success message appears along with the status of transaction.
    Click **OK** to complete the transaction.

47.4 Dashboard Overview – Design – Create Administrator Template

The system administrator can select a default dashboard available for administrator or can create a custom dashboard by dragging and dropping new widgets available from the list of components.

The administrator can create the administrator dashboard template either by selecting the administrative maintenance or group of administrative functions.

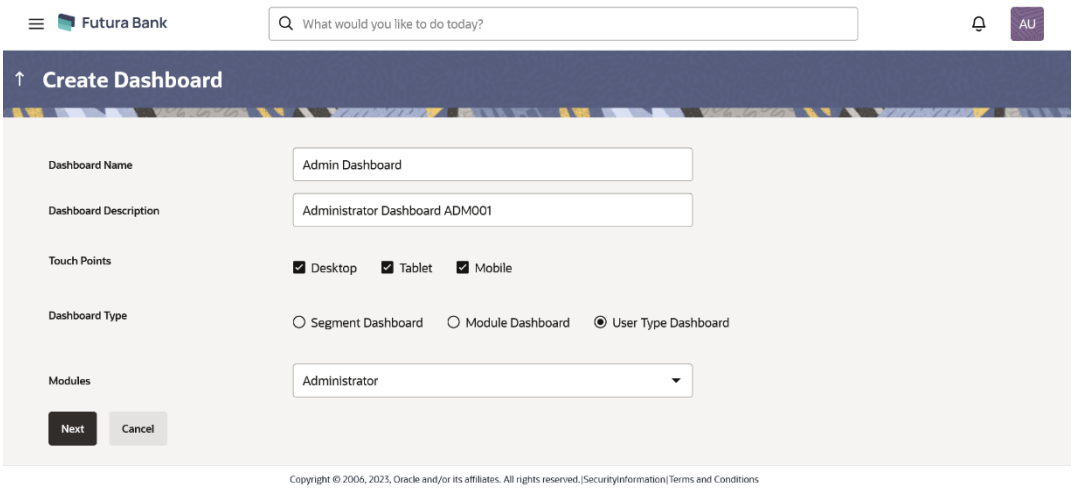
As part of administrative maintenances UI component, there are individual transaction quick links put in a single widget to component mapping available, the administrator user on actual login will be shown only those quick links that user has access to.

As part of system functions UI component, there is a logical group of transactions that can placed as a widget on the dashboard by selecting the administrative function from the group.

To create a new administrative dashboard template:

1. In the **Dashboard Overview** screen, click **Create**. The **Create Dashboard** screen appears.

Create Dashboard Template – For Administrator User Type



Field Description

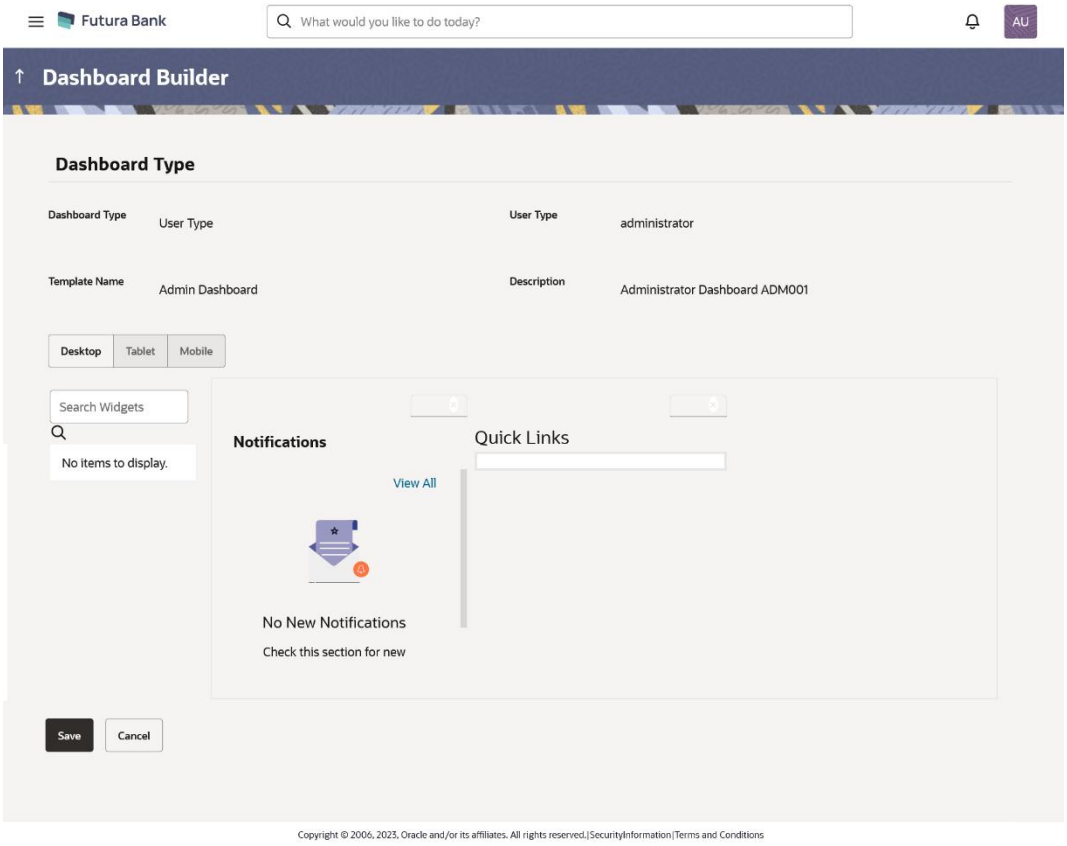
Field Name	Description
Template Name	Name of the template that the System Administrator user wants to create.
Template Description	Description for the template.
Design	The type of device on which the template will be enabled.
Select Module	System lists the dashboard for the segments / user type / module depending on the option selected.
User Type	Select administrator from the user type list.
List of Dashboards	System displays the list of dashboards available for selection based on the selected module type.

2. In the **Template Name** field, enter the name of the new template that is to be created.
3. In the **Template Description** field, enter the description of the new template.
4. To enable the template for Desktop/ Tablet / Mobile, select the required options from the **Design** check box.
5. From the **Segment Dashboard/ Module Dashboard/ User Type Dashboard** tabs, select the appropriate module. The **Dashboard Overview - Design** screen of the selected module

appears.
To customize the dashboard for an existing administrator user will need to select User Type Dashboard tab.

6. In the **User Type** field, select the administrator user.
7. Select the appropriate dashboard from the list of dashboards displayed based on the selected module.
8. Click **Next**. The **Dashboard Overview - Design** template for Administrator appears.
   OR
   Click **Cancel** to cancel the transaction and navigate to the 'Dashboard'.

Dashboard Overview - Design – Create Administrator Template

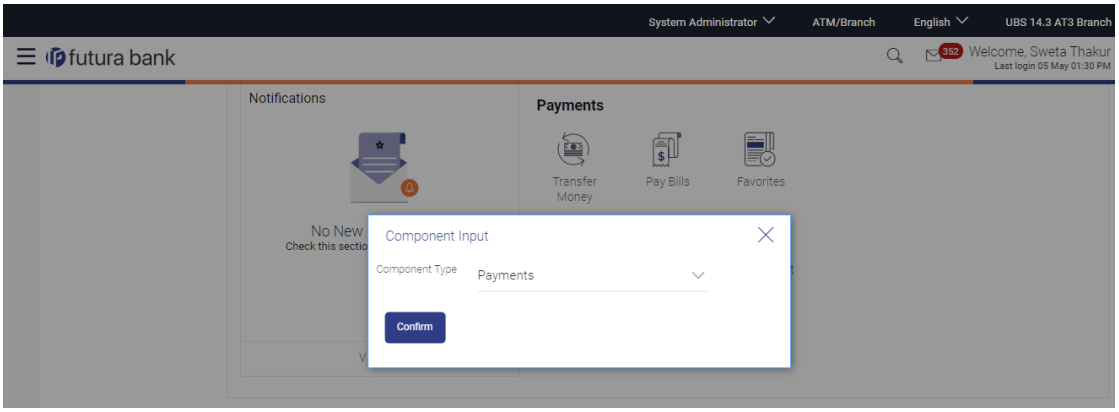


9. Click on the desired widgets from the widget list to appear on the dashboard.
   OR
   In the **Search Widget** field, enter the name of the widget that you want to appear on the dashboard and click .
   OR
   Click on the desired widgets of the dashboard to the desired location. System highlights the area where the widget can be placed.
10. Click on the upper right corner of the widget, if you want to expand the widget.
    OR
    Click on the upper right corner of the widget, if you want to compress the widget.

OR
Click ✕ on the upper right corner of the widget, if you want to remove the widget from the dashboard.

11. If the selected widget has multiple widgets on the same component like 'System Administrator Action Card', select the required widget that you want to appear on the dashboard.

Dashboard Overview - Component Input box



Field Description

Field Name	Description
Component Type	Select the component type, which you want to appear on your dashboard. This field is applicable only if the selected widget has multiple components.

m. From the **Component Type** list, select the widget component that you want to appear on the dashboard.

n. Click **Confirm**. The selected component appears as a widget on the selected location of your dashboard.

12. Click **Save** to save the template.
OR
Click **Cancel** to cancel the transaction and navigate to the 'Dashboard'.
OR
Click **Back** to navigate to previous screen.

13. The **Review** screen appears. Verify the details, and click Confirm.
OR
Click **Cancel** to cancel the transaction and navigate to the 'Dashboard'.
OR
Click **Back** to navigate to previous screen.
OR
Click the **Desktop**/ **Tab**/ **Mobile** icon to review the template in desktop, tab or mobile mode.

14. The success message appears.
    Click **Go to Dashboard** to view your customized dashboard.

47.5 Dashboard Overview – Edit

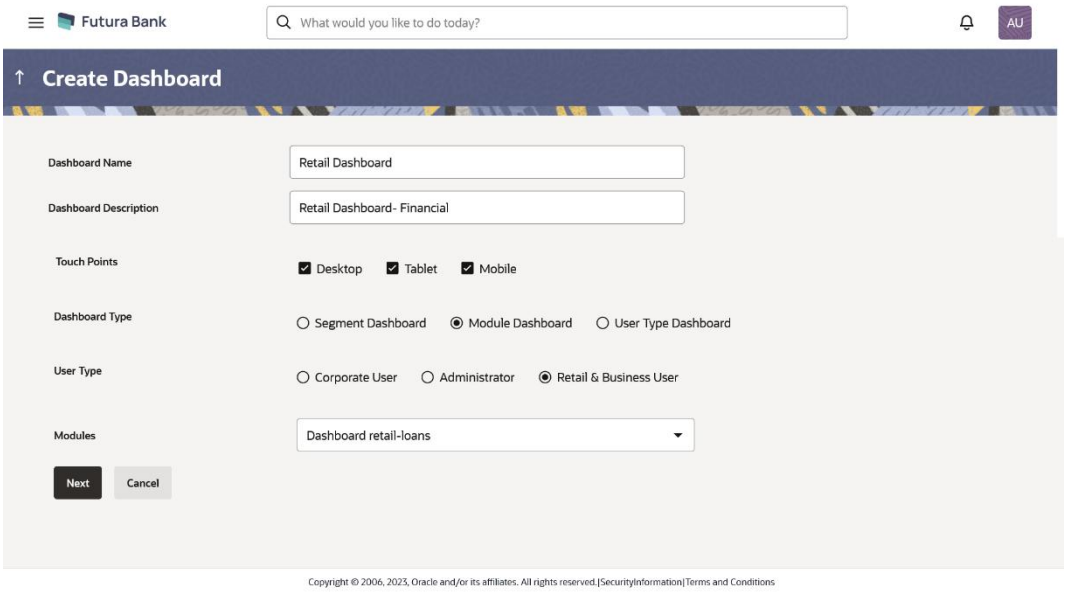
The system administrator can modify the configured dashboard using the **Edit** option. The administrator can edit the dashboard widgets for desktop, tablet or mobile devices by clicking the specific icons.

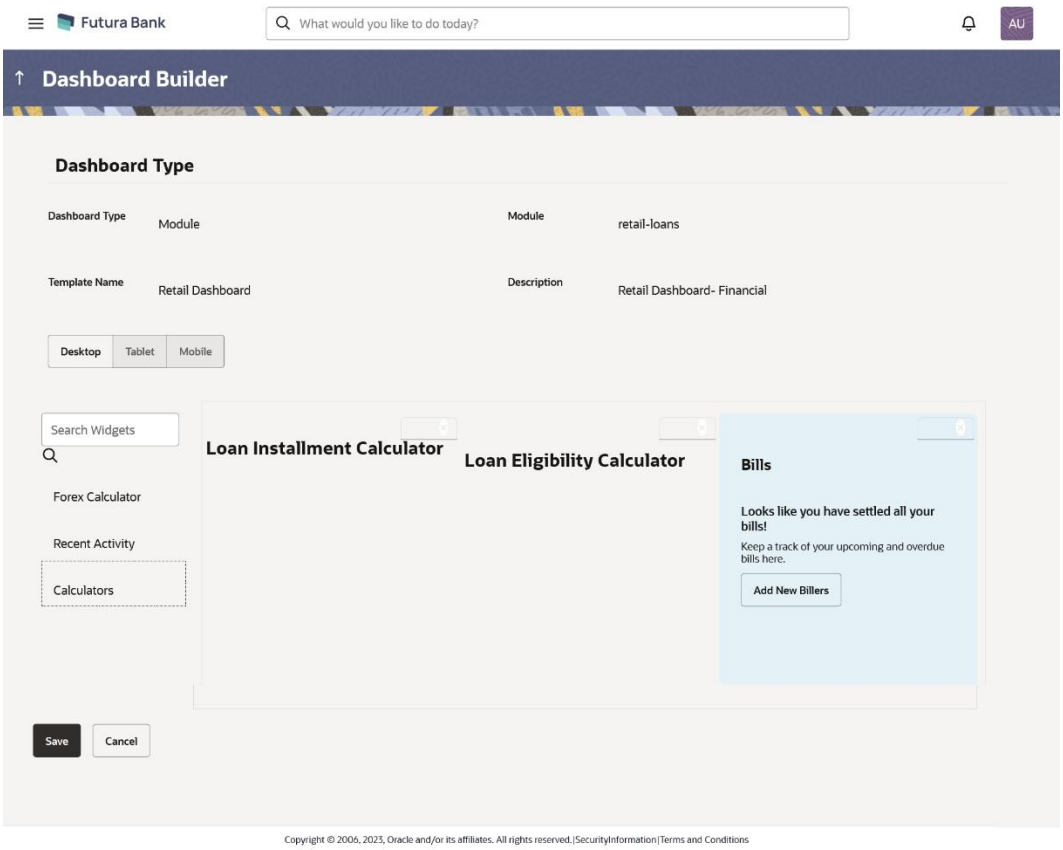
Note:
1) Dashboard Overview - Edit section is common for Administrator user and business users.
2) System Administrator will not be able to edit the factory shipped dashboards.

To edit the configured dashboard:

1. On the **Dashboard Overview** screen, click on **View Dashboard** tab.
   The **Dashboard Overview** - **Dashboard Listing** screen appears.
2. In the **Dashboard Overview** - **Dashboard Listing** screen, select the appropriate type of user in the **User Type** field. All the dashboard templates of the selected user type appears on the screen.
   OR
   In the **Template Name** field, enter the name of the template that you want to search. The searched dashboard template appears on the screen.
3. In **Action** column against the already created dashboard template, click on the icon, and then click **View/Edit Dashboard** link to edit the dashboard template details.
   The **Dashboard Overview - View Dashboard** screen appears.
   OR
   Click **Create Dashboard** to create a new dashboard template.
   OR
   Click **Back** to navigate to the previous screen.
4. Click the **Edit** link to modify the dashboard template. The **Dashboard Listing – Edit Dashboard** screen appears in edit mode.
   OR
   Click the **Desktop**/ **Tablet**/ **Mobile** icon to edit the template in desktop, tablet or mobile mode.
   OR
   Click **Cancel** to cancel the transaction.

Edit Dashboard Template





5. Click on the desired widgets from the widget list to add if required.
6. Click on the upper right corner of the widget, if you want to expand the widget.
   OR
   Click on the upper right corner of the widget, if you want to compress the widget.
   OR
   Click on the upper right corner of the widget, if you want to remove the widget from the dashboard.
7. Click **Save** to save the changes.
   OR
   Click **Cancel** to cancel the transaction and navigate to the 'Dashboard'.
   OR
   Click **Back** to navigate to previous screen.
8. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click the **Desktop**/ **Tablet**/ **Mobile** icon to review the template in desktop, tablet or mobile mode.
   OR
   Click **Edit** to make the changes if any for the selected device type.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
9. The success message appears along with the status of transaction.
   Click **Ok** to complete the transaction.

47.6 Dashboard Overview – Clone

To speed up the process of creating new dashboard template, System Administrator can clone an existing dashboard template. All the values available in an existing dashboard template are shown in an editable format, administrator is allowed to make changes in it and save the dashboard template with different name.

Following types of dashboard can be created:

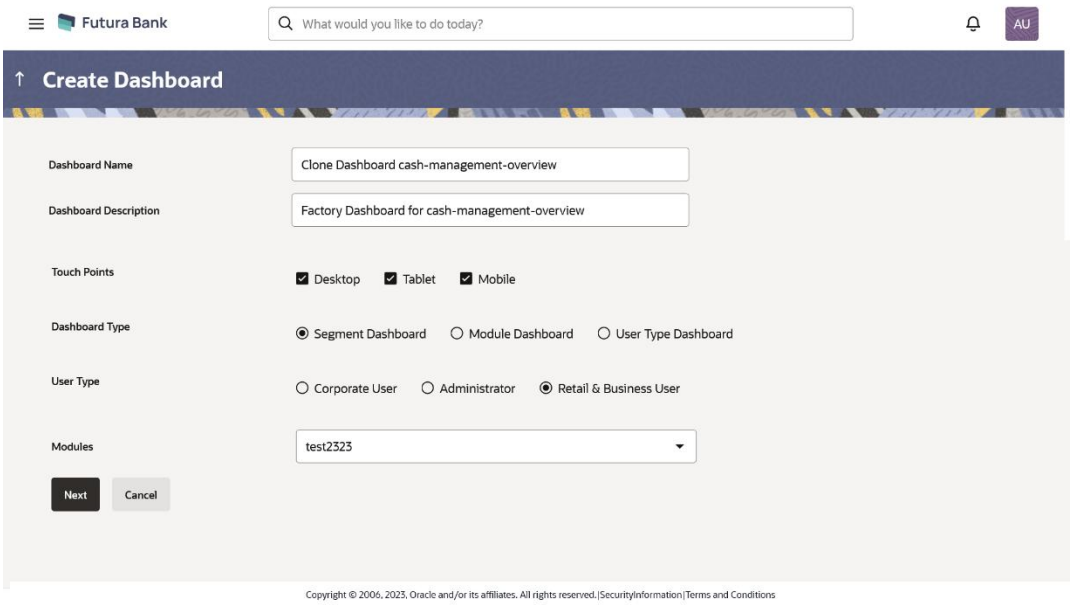
- Segment Dashboard - Design dashboard for a user segment
- Module Dashboard - Design dashboard for the available application modules i.e. CASA, Term Deposit, Loans etc.
- User Type Dashboard - Design dashboard for a user type i.e. Retail & Business, Corporate or Administrator.

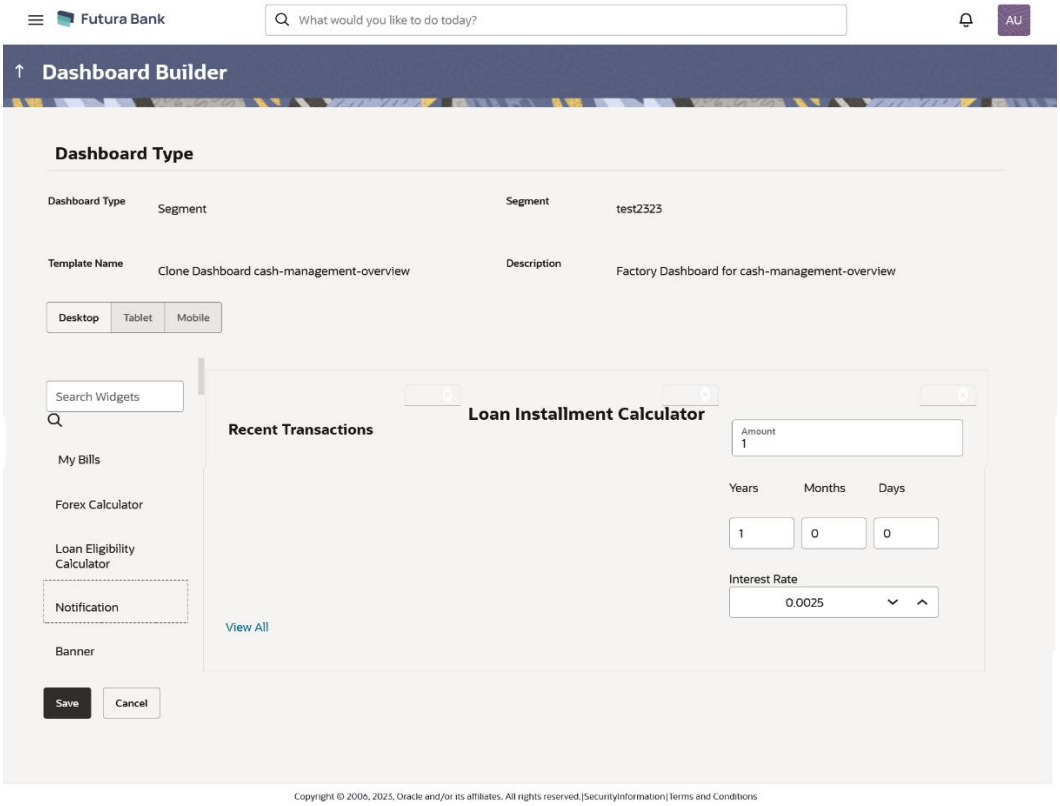
To clone a new dashboard template:

1. On the **Dashboard Overview** screen, click on **View Dashboard** tab.
   The **Dashboard Overview – Dashboard Listing** screen appears.
2. In **Action** column against the already created dashboard template, click on the icon, and then click **Clone Dashboard** link to clone the dashboard template details.

3. The **Dashboard Overview – Create** screen appears with existing dashboard template details.

Clone Dashboard Template





4. Update dashboard template with required changes.
5. Click **Save** to save the template.
   OR
   Click **Cancel** to cancel the transaction and navigate to the 'Dashboard'.
   OR
   Click **Back** to navigate to previous screen.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click the **Desktop**/ **Tab**/ **Mobile** icon to review the created template in desktop, tab or mobile mode.
   OR
   Click **Cancel** to cancel the transaction.
   A warning message of cancelling the operation appears. Click **Yes** to confirm.
   OR
   Click **Back** to navigate to previous screen.
7. The success message appears along with the status of transaction.
   Click **OK** to complete the transaction.

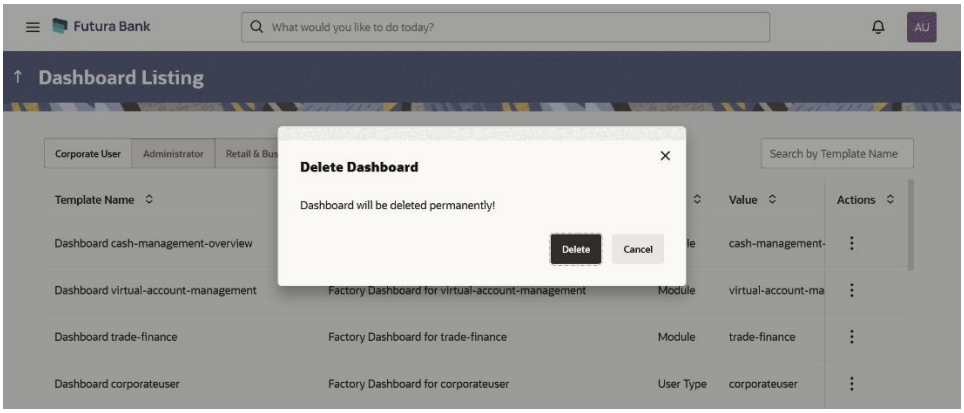
47.7 Dashboard Overview – Delete

The System Administrator can delete the custom dashboard templates maintained in the application. Deleting specific template will also result in deleting the template and revert back to the default dashboard.

To delete the configured dashboard:

1. Navigate to the **Dashboard Overview - Dashboard Listing** screen.
2. In **Action** column against the already created dashboard template, click on the ⋮ icon, and then click **Delete Dashboard** link to delete the existing dashboard template.
   The **Delete Dashboard** popup window appears.
   OR
   Click **Create Dashboard** to create a new dashboard template.
   OR
   Click **Back** to navigate to the previous screen.

Dashboard Builder - Delete



3. The application prompts the administrator with a warning message 'Dashboard will be deleted permanently' with an option of Delete / Cancel.
4. Click **Delete** to proceed with the deletion request.
   It will navigate to confirmation page with a success message along with the status and reference number.
   OR
   Click **Cancel** if you do not wish to proceed with deletion.
5. Click **OK** to complete the transaction.

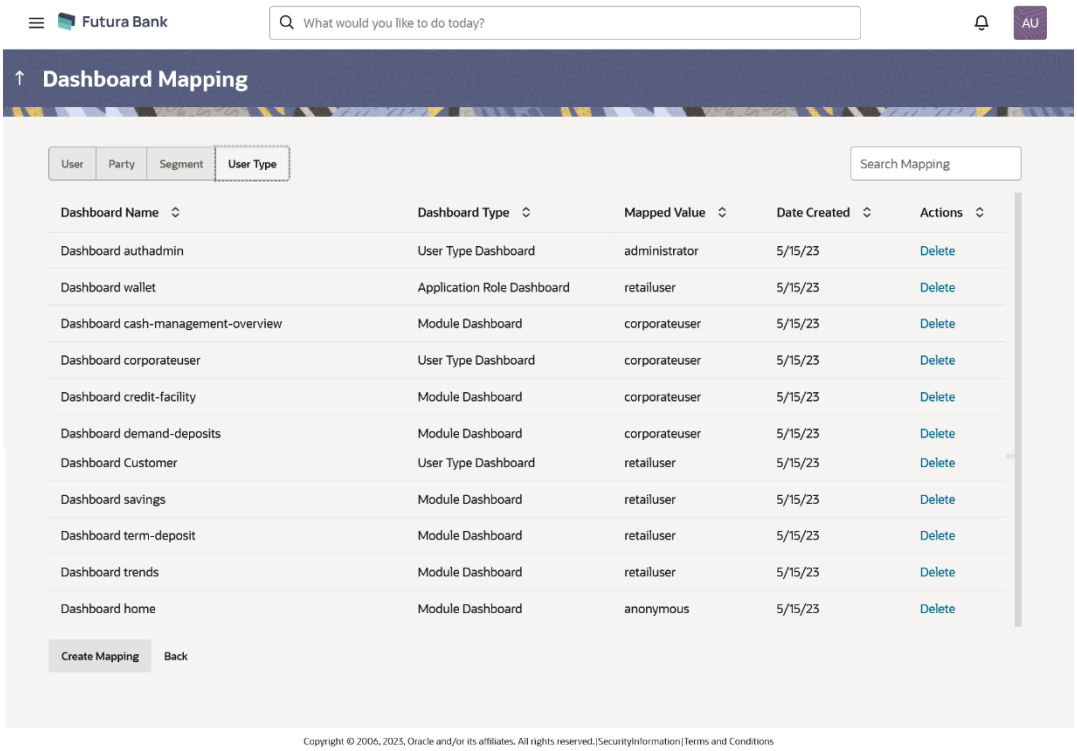
47.8 Dashboard Mapping – Summary

Using this option, System Administrator can map the configured dashboards to the user or party, or user type or user segments depending on the dashboard template selected. The system administrator can create mapping and can delete the mapping.

To view the Dashboard mapping summary:

1. Navigate to the screen, the **Dashboard Overview** screen appears.
2. In the **Dashboard Overview** screen, click the **View Mapping** tab. The **Dashboard Overview - Mapping** summary screen appears.

Dashboard Mapping Summary



Field Description

Field Name	Description
Mapping Type	Select the mapping type to search the dashboard template. The options are: • User • Party • Segment • User Type
Dashboard Name	System displays the name of the dashboard template.
Dashboard Type	System displays the type of the dashboard i.e. module / user type.
Mapped Value	System displays the value that is mapped to the template. In case if the dashboard is mapped to the user, user ID to whom the dashboard is mapped will be shown as mapped value. In case if the dashboard is mapped to the party, party ID to whom the dashboard is mapped will be shown as mapped value.
Date Created	The date on which template mapping was created.
Actions	Link to delete the mapping.

3. From the **Mapping Type** list, select the appropriate option for which you want to view the mapping. The **Dashboard Builder - Mapping Summary** screen appears.

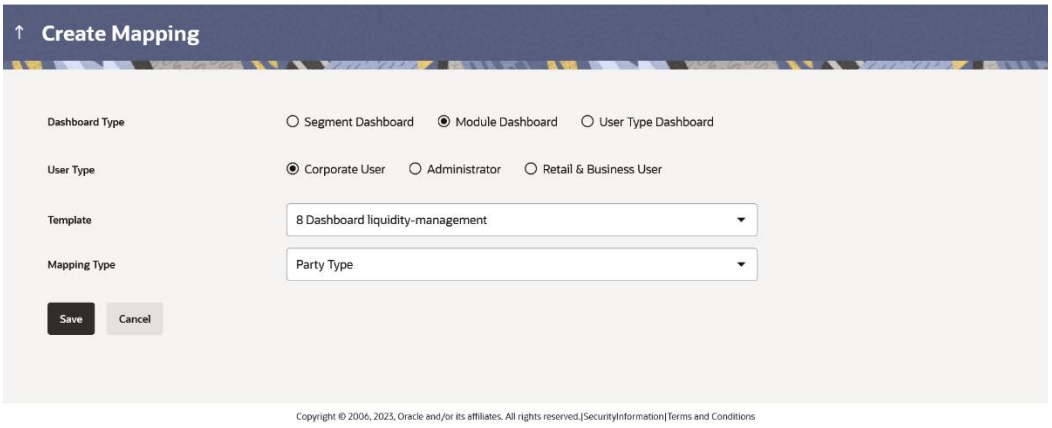
47.8.1 Create Mapping

Using this option, System Administrator selects the dashboard type, the dashboard template and then map either to a user/party/user segment/user type. The mapping type will depend on the type of dashboard selected.

To map dashboard templates:

1. In the **Dashboard Overview - Mapping** tab, click **Create Mapping**. The **Dashboard Overview - Create Mapping** screen appears.

Create Mapping



Field Description

Field Name	Description
Dashboard Type	Select the dashboard type that is to be mapped.
User Type	Select the user type for which the dashboard template needs to be mapped.
Template	Select the template from the list that needs to be mapped.
Mapping Type	Select the mapping type i.e. the selected dashboard template to map to the required option. The options are: • User • Party • Segment • User Type The mapping type options will also depend on the dashboard type selected i.e. for user type dashboard, system will not have options of User, Party and Segment
Mapping Value	The mapping value will depend on the option selected in the mapping type. For Party selected in the mapping type, the admin can capture the party for which the dashboard template is applicable. For user selected in the mapping type, the admin can capture the user for which the dashboard template is applicable. For segment selected as the mapping type, admin can capture the segment for which the dashboard template is applicable.

Field Name	Description
Party ID	Party Id to search a party that is to be mapped to the dashboard template. This field appears if you select **Party** option from the **Mapping Type** list.
Party Name	Party name to search a party that is to be mapped to the dashboard template. This field appears if you select **Party** option from the **Mapping Type** list.
User ID	User ID that is to be mapped to the dashboard template. This field appears if you select **User** option from the **Mapping Type** list.
Select Segment	Select the user segment that is to be mapped to the dashboard template. This field appears if you select **Segment** option from the **Mapping Type** list.

2. From the **Dashboard Type,** select the appropriate dashboard type i.e. Segment Dashboard or Module Dashboard or User Type Dashboard.
3. From the **User Type**, select the user type for which the Template mapping needs to be done.
4. Select the **Template** from the list that needs to be mapped.
5. From the **Mapping Type** list, select the appropriate option to be mapped.
   a. If you select **User** option, enter the user name.
   b. If you select **Party** option, enter the party Id in the **Party ID** field, and click **Search**.
   The Mapping Value appears.
   Click link under the Party ID column to view the party details.
   OR
   In the **Party Name** field enter the party name and click Search. The Mapping Value appears.
   Click link under the Party ID column to view the party details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the entered value.
   c. If you select **Segment** option, select the role from the **User Segment** list.
6. Click **Save**.
   The success message along with the status of transaction appears.
   OR
   Click **Cancel** to cancel the transaction.

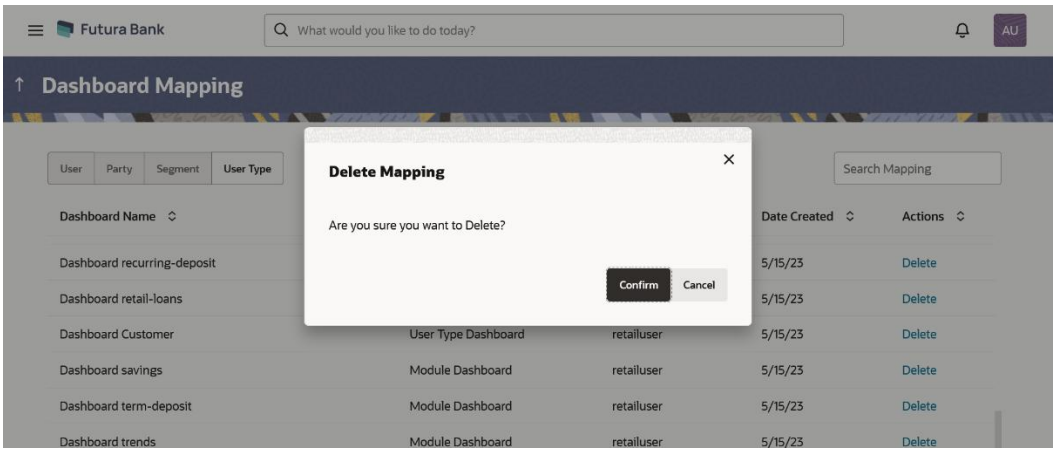
47.8.2 Delete Mapping

Using this option System Administrator can delete the templates mapped to a User or Party or User Segment or to a User Type.

To delete the mapped dashboard template:

1. In the **Dashboard Overview** screen, click the **View Mapping**. The **Dashboard Overview - Mapping** summary screen appears.
2. Click on the **Mapping** tab.
3. Select the **Mapping Type** from the list i.e. User / Party / Segment / User Type.
4. In the **Action** column, click **Delete** against the template mapping that you want to delete. The application will prompt the administrator with a deletion message with an option of Confirm/ Cancel.

Delete Mapping



5. Click **Confirm** to delete the mapping. It will navigate to confirmation page with a success message and the status.
   OR
   Click **Cancel** if you do not wish to delete the mapping.
6. Click **OK** to complete the transaction.

FAQ

1. **Can I design new widgets using Dashboard Overview functionality?**

   No, designing of a new widget is not allowed using this functionality. Administrator can use the existing widgets and can design the required dashboard.

2. **Can I design different dashboards for different device types (desktop, mobile and tablet) using one template?**

   Yes, you can design different dashboards for different types of devices using one template. An edit option is available while previewing the dashboard on each type of device, which will help the user to make the necessary changes for specific device type.

3. **Can I delete the template that is mapped to a user / party / segment / user type?**

Yes, you can delete the template that are already mapped to a user / party / segment or user type. A warning message informing about the mapping deletion is shown to the administrator while deleting a template.

4. Can I map the same template to multiple users or parties?

Yes, you can map the same template to multiple parties or users. Separate entries are required for such mapping.

5. Can the system/bank administrator edit a Factory shipped dashboard ?

No, Factory shipped dashboards can't be modified. However system/bank administrator can modify a custom made dashboard.an I design the dashboard and map for administrator types of users (Bank/system administrator and corporate administrator)?

6. Can I design a dashboard for System Admin or Bank Admin?

Yes, you can design the administrative dashboards using Dashboard Builder maintenance.

7. When will the newly mapped dashboard be visible to the end customer?

Newly mapped dashboard will be available to the end user with an immediate effect.

8. Can an end user (Retail & Business /Corporate users) design their own dashboards or set their preferences to see required widgets?

Yes Retail & Business and Corporate users can personalize and design their dashboard.

9. In case of dashboard templates available at user level, segment level, and user type level, which dashboard will the system resolve? Also what is the order in which the dashboards are resolved?

If there is a dashboard template mapped at a user level, then the system will display the user level dashboard on login.

Before rendering the dashboard, system will first check if there is a dashboard at user level, followed by segment, and then at user type.

In case where a retail & Business user has personalize his/her dashboard, the system will give the priority to user defined dashboard followed by Administrator defined dashboards as user, segment, and then at user type.

48. Relationship Maintenance

Customer Relationship Maintenance enables the System Administrator to set up the transaction access logic for Bank's retail customers from Digital Banking Platform based on their account - mode of operation or relationship.

E.g. If a customer relationship (Mode of operation) is 'Either or Survivor', provide an access of all transactions whereas, if a customer relationship (Mode of operation) is 'Jointly', provide an access of all Inquiries and restrict all financial transactions from Digital Banking Platform. Such account and transaction access rules can be set up by the System Administrator using 'Relationship Maintenance Module'.

This account relationship maintenance is a two-step process.

- Relationship Mapping Maintenance - Using this maintenance System Administrator can map OBDX relationship codes with core banking relationship codes
- Relationship Matrix Definition - Using this maintenance System Administrator can define the transaction access based on the account relationships

48.1 Relationship Mapping

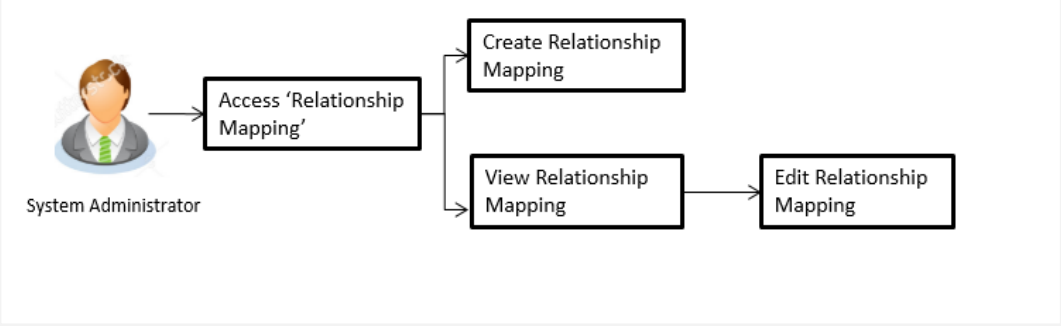
Using this option a System Administrator can map OBDX account relationship codes with account relationship codes defined in Core Banking Application so that the corresponding matrix defined in OBDX will be followed based on the available account relationship in the core application.

Note: The relationship matrix maintenance is done using **Relationship Matrix Maintenance** transaction.

Prerequisites

- Transaction access is provided to System Administrator.
- Account relationship codes are maintained in OBDX and in Core Banking Application.

Workflow



Features supported in application

The administrator can perform the following actions:

- Create Relationship Mapping
- Search/ View Relationship Mapping
- Edit Relationship Mapping

How to reach here:

System/ Bank Administrator Dashboard > Controls & Monitoring > Relationship Mapping
OR
System Administrator Dashboard > Toggle Menu > Menu > Controls & Monitoring > Relationship Mapping

48.1.1 Relationship Mapping Maintenance - View

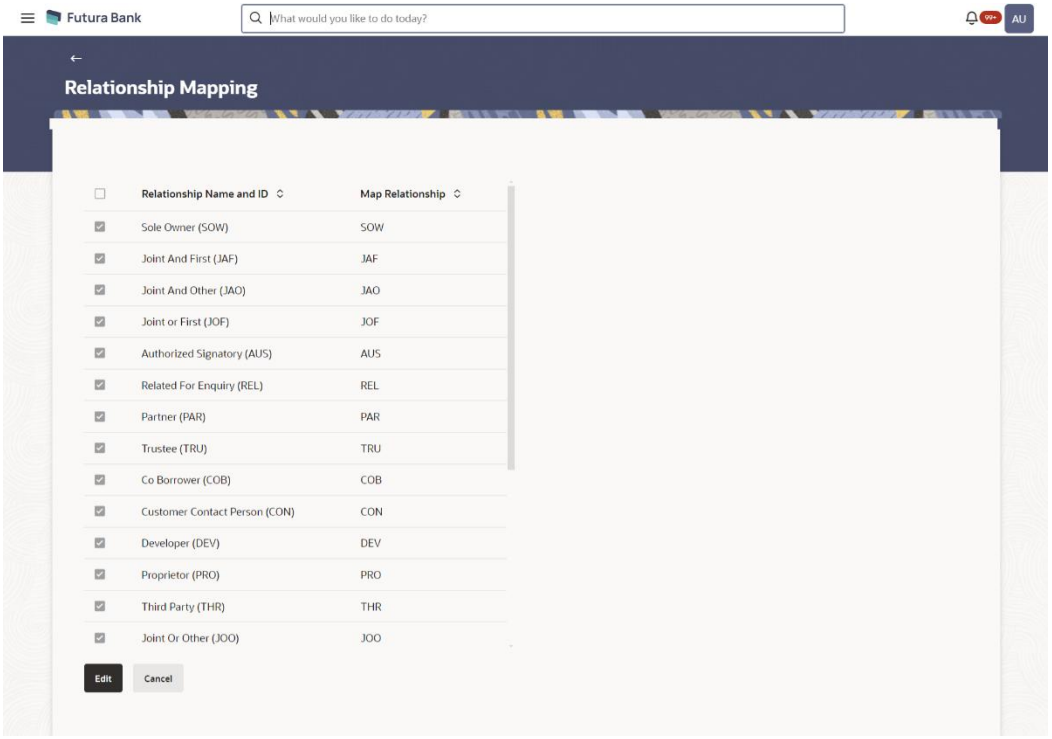
By accessing this menu option, System Administrator can view the account relationship codes maintained in OBDX and paired with the codes maintained in Core Banking Application

Relationship code maintained in OBDX appears on left side of the screen and paired codes if any appears on right side of the screen

1. All the relationships maintained under user account appears on **Relationship Mapping Maintenance** screen.
   OR
   Click **Edit** to edit the maintenance.
   OR
   Click **Cancel** to cancel the transaction.

Note: Instead of the **Edit** option, the **Save** option available if user is accessing it for the first time.

Relationship Mapping Maintenance



Field Description

Field Name	Description
Relationship Name and ID	Lists all the relationships maintained in OBDX.
Map Relationship	Lists all the relationships maintained in Core Banking Application.

48.1.2 Relationship Mapping Maintenance - Edit

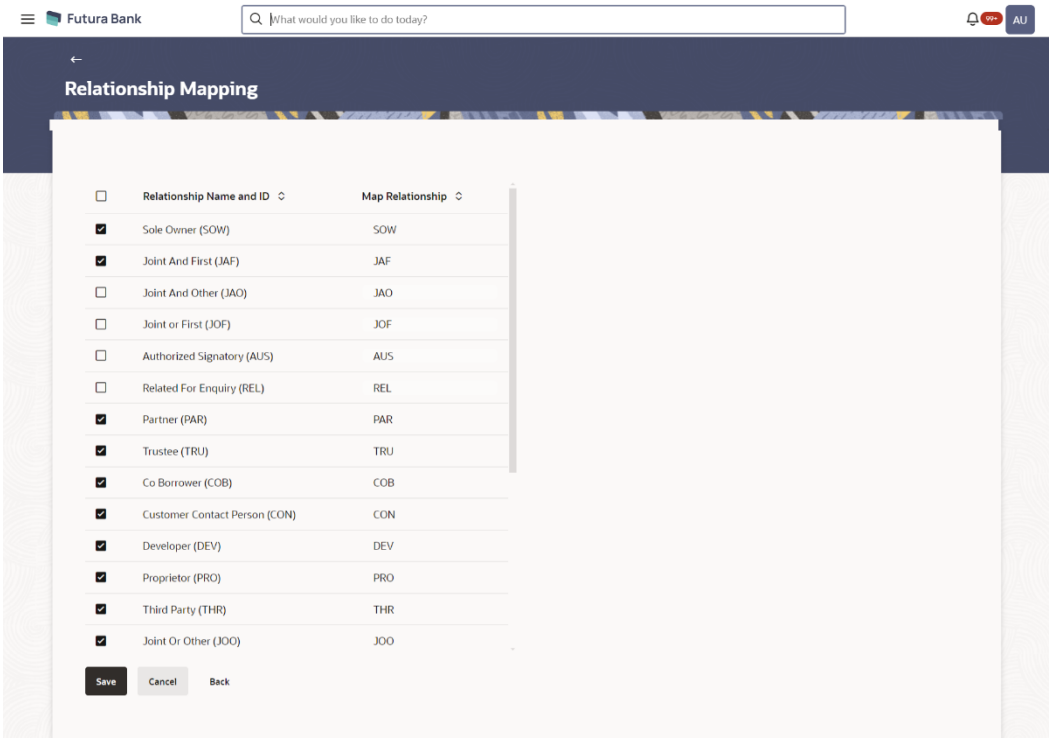
Using this option, System Administrator is allowed to map the newly added relationship codes with the codes defined in core application. As well as System Administrator can remove the relationship codes which are selected from the default list.

To modify relation mapping:

1. Navigating to **Relationship Mapping Maintenance** screen, application displays the All the relationships maintained under user account.

2. Click **Edit** to edit the maintenance.
   OR
   Click **Cancel** to cancel the transaction.

Relationship Mapping Maintenance - Edit



Field Description

Field Name	Description
Relationship Name and ID	To map the OBDX relationships with the relationship codes available in the Core Banking system. **Note:** Lists all the relationships maintained in OBDX.
Map Relationship	Relationship ID to be mapped with OBDX relationship ID. **Note:** Lists all the relationships maintained in Core Banking Application. If an existing mapping is available, a value will be shown in **Map Relation** field.

1. Select the checkbox against **Relationship Name and ID** to map Core Banking relationships to OBDX relationships.

Note:
1) Select the checkbox adjacent to **Relationship Name and ID** in header row to select all relationships in one instance.
2) To unmap the relation mapping, uncheck the checkbox

2. In the **Map Relationship** field, enter the relationships value as maintained in Core Banking Application.
3. Click **Save** to save the relationship mapping maintenance.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
4. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
5. The success message of Relationship Mapping Maintenance saved successfully appears along with the transaction reference number.
   Click **OK** to complete the transaction.

48.2 Relationship Matrix

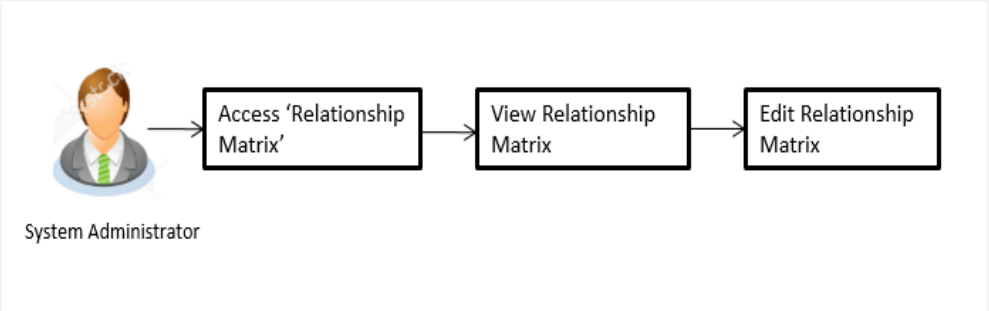
Relationship Matrix maintenance allows the System Administrator to define the transaction access based on the account relationships. Administrator can enable or disable each transaction for each relationship code.

OBDX first checks if the transaction is mapped to the role attached to the user and then if it is enabled in relationship matrix. If both the conditions are satisfied, an access of a transaction and of an account is provided to the user.

Prerequisites

- Transaction access is provided to System Administrator.
- Approval rule set up for System Administrator to perform the actions.
- Account relationship codes are maintained in OBDX and in Core Banking Application.
- Relationship mapping (mapping of OBDX relationship codes with codes maintained in Core Banking application) is maintained.

Workflow



Features supported in application

The administrator can perform the following actions:

- View Relationship Matrix
- Edit Relationship Matrix

How to reach here:

System/ Bank Administrator Dashboard > Controls & Monitoring > Relationship Matrix
OR
System Administrator Dashboard > Toggle Menu > Menu > Controls & Monitoring > Relationship Matrix

48.2.1 Relationship Matrix Maintenance - View

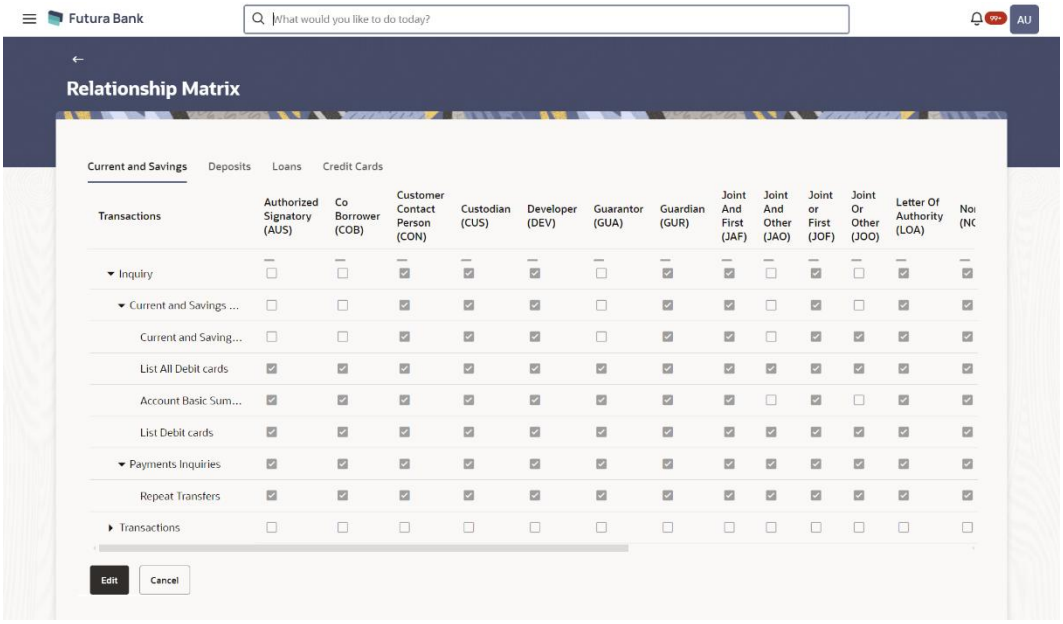
Based on the account relationship and transaction access matrix, System Administrator will know the account relationships IDs for which the channel access has been granted.

To view relationship matrix:

1. Displays the details maintained under user account relationship and transaction access matrix in **Relationship Matrix Maintenance - View** screen.
   OR
   Click **Edit** to modify the maintenance.
   OR
   Click **Cancel** to cancel the transaction.

Note: Instead of the **Edit** option, the **Save** option available if user is accessing it for the first time.

Relationship Matrix Maintenance - View



Field Description

Field Name	Description
Module Name	Name of the module under which all transactions are maintained for Relationship Matrix. • Current and Savings • Deposits • Loans • Credit Cards

Field Name	Description
Transaction Name	Lists all the transactions under a specific module for which a channel access has been granted based on account relationship and transaction access matrix. Under each module transactions are mainly grouped as: • Inquiry • Transactions
Relationship ID	Lists all the relationship IDs maintained in OBDX for which the codes available in core banking application are mapped.

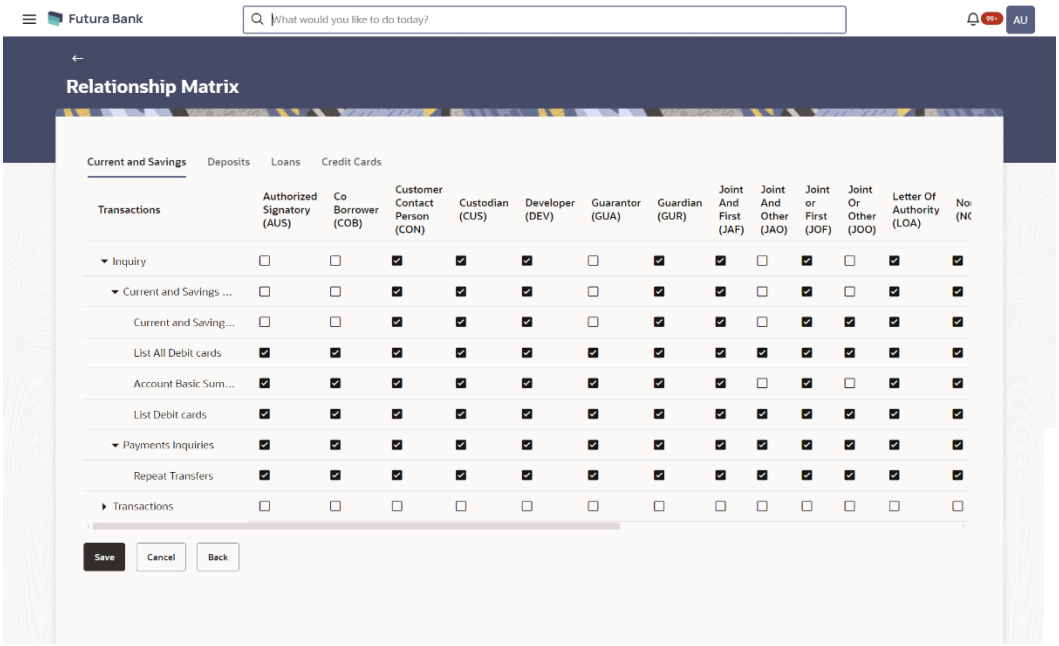
48.2.2 Relationship Matrix Maintenance - Edit

Using this option, System Administrator can modify the account relationship and transaction access matrix.

To modify relationship matrix:

1. Displays the details maintained under user account relationship and transaction access matrix in **Relationship Matrix Maintenance - View** screen.
2. Click **Edit** to modify the maintenance.
   The **Relationship Matrix Maintenance - Edit** screen appears.

Relationship Matrix Maintenance - Edit



Field Description

Field Name	Description
Module Name	Name of the module under which all transactions are maintained for Relationship Matrix. • Current and Savings • Deposits • Loans • Credit Cards
Transaction Name	Lists all the transactions of a specific account for which a channel access has been granted based on account relationship and transaction access matrix. The transaction categories are: • Inquiry • Transactions Select/ deselect the transactions to maintain relationship matrix.
Relationship ID	Lists all the relationship IDs maintained in OBDX for which the codes available in core banking application are mapped.

3. Select the check box available in the header of transaction category (Inquiry and Transactions**),** to select all transactions for selected category in one instance.
   OR
   Select the check box available against the **Relationship ID**) for each transaction.

Note:
1) Select / deselect the check box against the Transaction category (Inquiry and Transactions) to select all transactions under it.
2) To unmap the relation mapping, deselect the check box.

4. Repeat step 2 for all modules as per requirement.
5. Click **Save** to save the relationship matrix maintenance.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to the previous screen.
6. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to previous screen.
7. The success message of Relationship Matrix Maintenance saved successfully appears along with the transaction reference number.
   Click **OK** to complete the transaction.

FAQ

1. **Is relationship mapping a mandatory step?**

   Yes, relationship mapping is a mandatory step, without which the accounts will not be fetched from the core banking application.

2. **Will all transactions available be listed under a respective module on relationship matrix screen?**

   Transactions for which the Customer Relationship Matrix maintenance flag is enabled in 'Transaction Aspects' screen will be listed under the respective modules.

3. **Will a user get the access of a transaction and of an account, based on the relationship matrix definition?**

   No, OBDX first checks if the transaction is mapped to the role attached to the user and then if it is enabled in relationship matrix. If both the conditions are satisfied, access of the transaction and of account is provided to the user.

4. **What will happen if an inquiry access for current and savings accounts module have been granted for a specific relationship code e.g. JAF (Joint and First) and not provided for a non-inquiry transactions?**

   In the above case user having an account with the relationship code JAF, will be able to access all inquiry transactions from digital platform but the account will not be listed in non-inquiry transaction screen.

49. Transaction Blackout

A blackout period is duration of time when access to something usually available is prohibited.

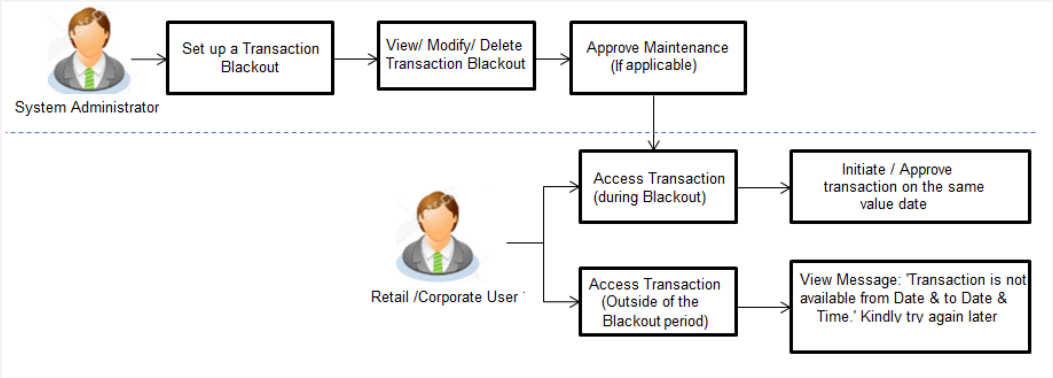
When a System Administrator maintains a transaction blackout, for a period, transaction/s are not accessible to users of the bank's retail and corporate or even to the administrator users for a preset time period.

The system administrator may use the time, when a transaction is blacked-out, to do necessary maintenances.

Pre-Requisites

- Transaction access is provided to System Administrator.
- Approval rule set up for system administrator to perform the actions.

Workflow



Access Transaction (during blackout) – Blackout message needs to be displayed

Check the flow, message part is against access of transaction outside blackout period.

Features Supported In Application

The following options are available as part of this maintenance:

- Create a new Transaction Blackout Maintenance
- Search and View Transaction blackouts already maintained
- Delete or Edit transaction blackouts maintained.

How to reach here:

System/ Bank Administrator Dashboard > Controls & Monitoring> Transaction Blackout
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Controls & Monitoring> Transaction Blackout

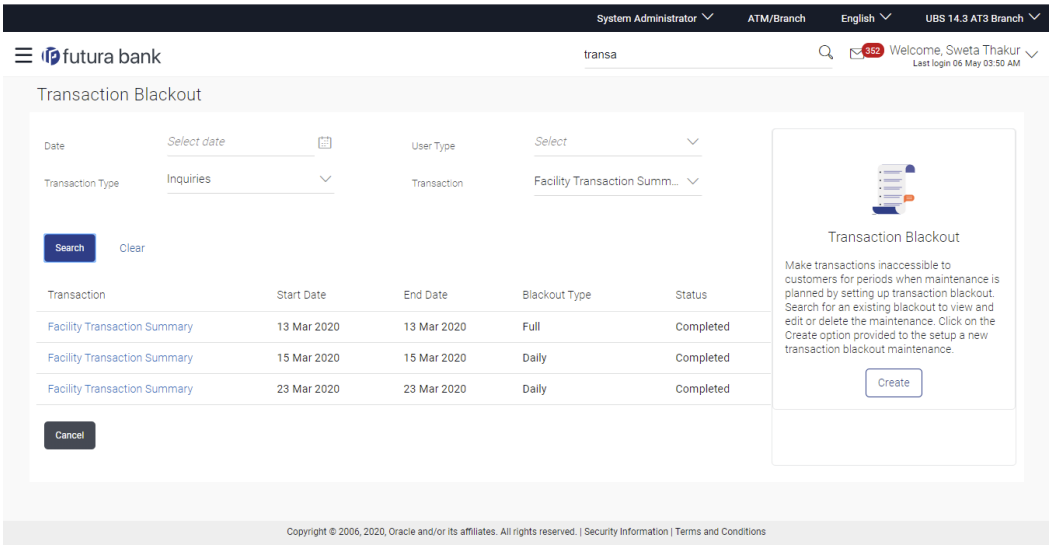
49.1 Transaction Blackout - Search

This function allows the System Administrator to search for transactions under a particular user type and also to create a new Transaction blackout. The search is available on the basis of User type, Transaction Type, Transaction and date. The search result displays only those transactions under a user type for which the 'Transaction Blackout' is maintained.

To search for transactions under a particular user type:

1. Enter the search criteria.
2. Click **Search**, displays results based on search criteria.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction.

Transaction Blackout- Search



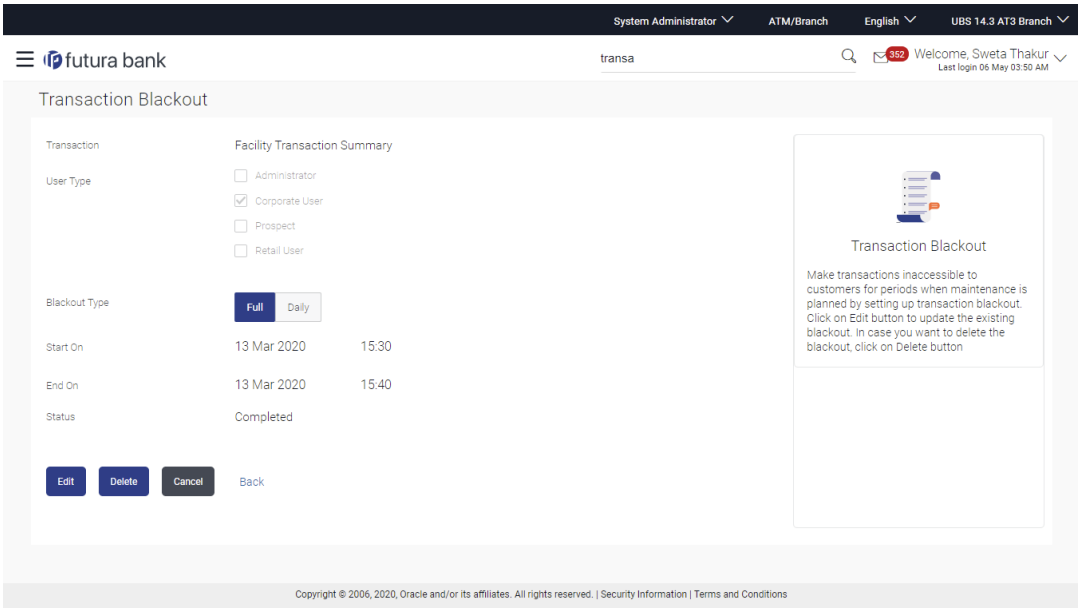
Field Description

Field Name	Description
Date	Date of the transaction blackout.

Field Name	Description
User Type	The type of user for whom the transaction is blacked out. The user types could be: • Corporate User • Administrator • Retail User Prospect
Transaction Type	Transaction type to be blacked out. The options are: • Maintenances • Administration • Inquiries • Non-Financial • Financial
Transaction	The specific transaction, for which a blackout is maintained. Transactions list displayed here gets populated basis on the transaction type selected in the previous field.
Search Result	
Transaction	The specific transaction, for which a blackout is maintained
Start Date	Start date for the blackout.
End Date	End date for the blackout.
Blackout Type	Type of black out. • Full: Indicates that it will be complete transaction blackout for the set date and time. • Daily: Indicates that it will be daily blackout for the set date and time.
Status	The transaction blackout status. The options are: • Ongoing: Indicates that blackout is ongoing. • Scheduled: Indicates that scheduled for some day in the future.

3. View the table with search results. This table contains the start date and end date of the blackout maintenance. Transaction for which the blackout is applicable, the type of blackout (full or daily) and the status – whether the blackout is ongoing, or scheduled for some day in the future.
4. Click on the field **Transaction** to view more details.

Transaction Blackout- View details



Field Description

Field Name	Description
Transaction	The specific transaction, for which a blackout is maintained.
User Type	The type of user for whom the transaction is blacked out. The user types could be: • Corporate User • Administrator • Retail User • Prospect
Blackout Type	Type of black out. • Full: Indicates that it will be complete transaction blackout for the set date and time. • Daily: Indicates that it will be daily blackout for the set date and time.

Field Name	Description
Start On	Start date and time for the blackout. This field will be displayed if the Blackout type is selected as '**Full**'.
End On	End date and time for the blackout. This field will be displayed if the Blackout type is selected as '**Full**'.
Date Range	Blackout start and end date. This field will be displayed if the Blackout type is selected as '**Daily**'.
Time Range	Blackout start and end time. This field will be displayed if the Blackout type is selected as '**Daily**'. **Note:** When blackout type is full - the following fields are displayed and enabled: Start On (Date and Time) End On and (Date and Time) When blackout type is Daily - the following fields are displayed and enabled - Date Range - From and To. Time Range - From and To. And, an option to Add Time
Status	The transaction blackout status. The options are: • Ongoing: Indicates that blackout is ongoing. • Scheduled: Indicates that scheduled for some day in the future.

5. Click **Edit** to edit the maintenance.
   OR
   Click **Delete** to delete the maintenance.
   OR
   Click **Cancel** to close the blackout creation process.
   OR
   Click **Back** to navigate to previous screen.

49.2 Transaction Blackout - Create

System Administrator can create new transaction blackout maintenance for the selected transaction. User needs to select the particular transaction and user type for whom blackout needs to be applied.

Further user can set up blackout type:

- Full – Black out for the entire period.
- Daily - Blackout between start and end time daily, for the days set.

To create new transaction blackout:

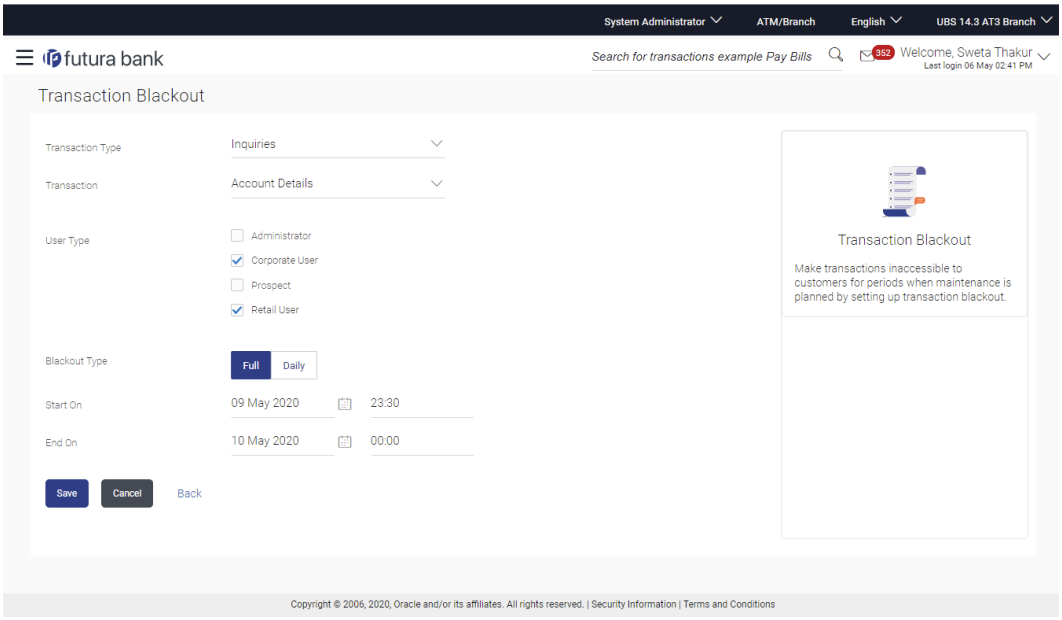
1. Click **Create**.
2. From the **Transaction** list select the appropriate option.

   Note :
   - You can select multiple transactions out of the listed transactions for setting up the blackout in one go.
   - There will be an option as 'All transactions' in the dropdown, on selecting the same all the listed transactions, will get selected for maintaining the blackout.

3. From the **User Type** select the appropriate option.
4. From the **Blackout Type** select the appropriate option:
5. If you select **Full Day:**
   a. From the **Start On** list, select the start date and time of the transaction blackout.
   b. From the **End On** list, select the end date and time of the transaction blackout.
6. If you select **Daily:**
   a. From the **Date Range** list select the start and end date of the transaction blackout.
   b. From the **Time Range** list select the start and end time of the transaction blackout.

Note: You can click **+Add Time Range** button, to add multiple time options for transaction blackout.

Transaction Blackout- Create



Field Description

Field Name	Description
Transaction Type	Transaction type to be blacked out. The options are: • Maintenances • Administration • Inquiries • Non-Financial • Financial
Transaction	The specific transaction, for which a blackout is to be maintained. Note : • You can select multiple transactions out of the listed transactions for setting up the blackout in one go. • There will be an option as 'All transactions' in the dropdown, on selecting the same all the listed transactions, will get selected for maintaining the blackout. • Selected transactions will go as an individual maintenance for approval (one approval for one transaction) • Selected transactions will be available as a single maintenance in view and edit. • Multiple selection would be available only at the time of set up. Maintained blackout can be inquired and edited only for one transaction at a time
User Type	The type of user for whom the transaction is blacked out. The user types could be: • Corporate User • Administrator • Retail User • Prospect
Blackout Type	Type of black out. • Full: A Full transaction blackout prevents access to a transaction from a certain day/time to certain day / time. The transaction is not enabled at all, during a full blackout • Daily: A daily transaction blackout prevents access to a transaction for the defined time in a day, over few days. The transaction is enabled, outside of the blackout window, in case of a daily blackout

Field Name	Description
Start On	Start date and time for the blackout. This field will be displayed if the Blackout type is selected as '**Full**'.
End On	End date and time for the blackout. This field will be displayed if the Blackout type is selected as '**Full**'.
Date Range	Blackout start and end date. This field will be displayed if the Blackout type is selected as '**Daily**'.
Time Range	Blackout start and end time. This field will be displayed if the Blackout type is selected as '**Daily**'.

Note:
When blackout type is full - the following fields are displayed and enabled: Start On (Date and Time) End On and (Date and Time) When blackout type is Daily - the following fields are displayed and enabled - Date Range - From and To. Time Range - From and To. And, an option to Add Time Range

7. Click **Save** to create the transaction blackout. User will be directed to the Transaction Blackout-Create - review page post necessary validations.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to previous screen.
8. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
9. The success message appears along with the transaction reference number. Click **Ok** to complete the transaction.

49.3 Transaction Blackout - Edit

System Administrator can modify existing blackout instructions. This screen displays the inputs captured for Daily/Full, End date and End time in the create transaction blackout screen in an editable form. Whereas user is not allowed to edit Transaction.

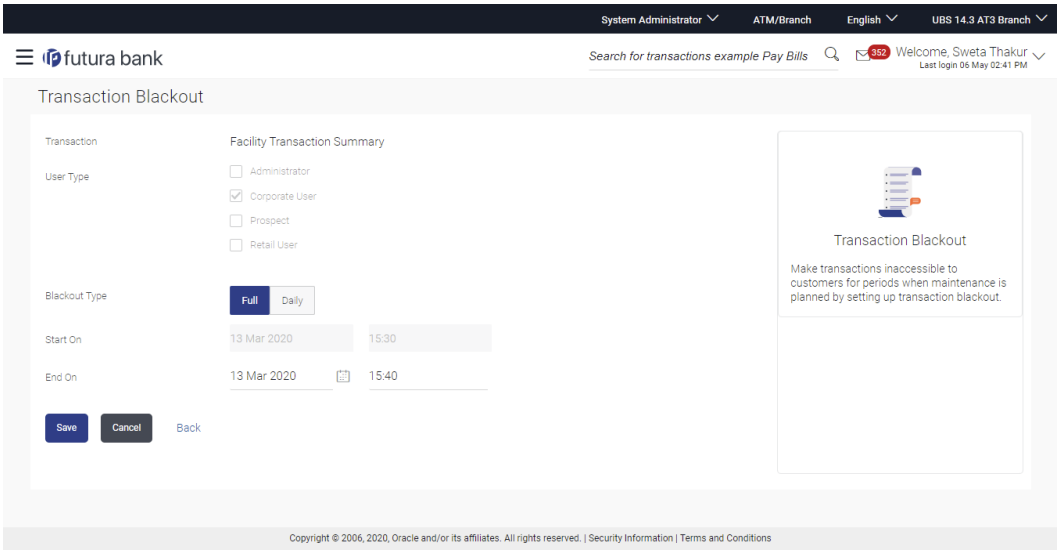
To modify blackout instructions:

1. Enter the search criteria like **Transaction**, **Date,** or **User Type**.

Note: Alternately, the user can perform a blank search.

2. Click **Search**, displays results based on search criteria.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction.
3. Click on the transaction.
4. Click **Edit** to edit the maintenance.

Editing a scheduled Maintenance



Field Description

Field Name	Description
Transaction	The specific transaction, for which a blackout is to be modified.
User Type	The type of user for whom the transaction is blacked out. The user types could be: • Corporate User • Administrator • Retail User • Prospect

Field Name	Description
Blackout Type	Type of black out. • Full: A Full transaction blackout prevents access to a transaction from a certain day/time to certain day / time. The transaction is not enabled at all, during a full blackout • Daily: A daily transaction blackout prevents access to a transaction for the defined time in a day, over few days. The transaction is enabled, outside of the blackout window, in case of a daily blackout
Start On	Start date and time for the blackout. This field will be displayed if the Blackout type is selected as '**Full**'.
End On	End date and time for the blackout. This field will be displayed if the Blackout type is selected as '**Full**'.
Date Range	Blackout start and end date. This field will be displayed if the Blackout type is selected as '**Daily**'.
Time Range	Blackout start and end time. This field will be displayed if the Blackout type is selected as '**Daily**'.

Note:
When blackout type is full - the following fields are displayed and enabled: Start On (Date and Time) End On and (Date and Time) When blackout type is Daily - the following fields are displayed and enabled - Date Range - From and To. Time Range - From and To. And, an option to Add Time Range

5. From the **User Type** select the appropriate option.
6. From the **Blackout Type** select the appropriate option:
7. If you select **Full Day:**
   a. From the **Start On** list, select the start date and time of the transaction blackout.
   b. From the **End On** list, select the end date and time of the transaction blackout.
8. If you select **Daily:**
   a. From the **Date Range** list, select the start and end date of the transaction blackout.
   b. From the **Time Range** list, select the start and end time of the transaction blackout.

Note: You can click **+Add Time Range** button, to add multiple time options for transaction blackout.

9. Click **Save** to button to save Transaction Blackout Maintenance. User is directed to **Transaction Blackout-Edit - review** page post necessary validations.
   OR
   Click **Cancel** to cancel the transaction.

OR
Click **Back** to navigate to the previous screen.

10. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to the previous screen.
11. The success message appears along with the transaction reference number. Click **OK** to complete the transaction.

49.4 Transaction Blackout - Delete

System Administrator can delete existing blackout instructions. User is allowed to delete future dated blackouts. Deleting ongoing blackout will stop the blackout and the transaction will be available to the users post approved by necessary levels of approvals.

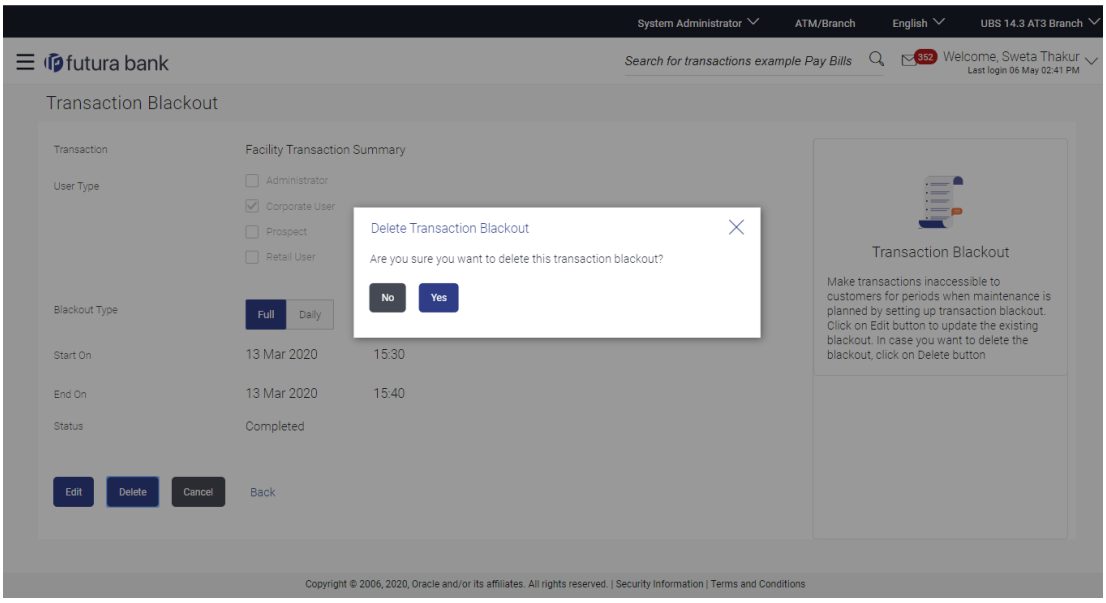
To delete maintenance:

1. Enter the search criteria like **Transaction**, **Date,** or **User Type**.

Note: Alternately, the user can perform a blank search.

2. Click **Search**, displays results based on search criteria.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction.
3. Click **Edit** to edit the maintenance.
   OR
   On the Detailed View screen, click **Delete** to delete the maintenance.
   OR
   Click **Cancel** to close the blackout creation process.
   OR
   Click **Back** to navigate to previous screen.
4. The Pop-up Message to confirm deletion appears.

Deleting an Ongoing / scheduled Maintenances



5. On the Detailed View screen, of the blackout, click **Delete**.
6. The Pop-up Message to confirm deletion appears.
7. Click **Yes** to delete.
   OR
   Click **No** to go back to the maintenance.
8. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
9. The success message appears along with the transaction reference number. Click **Ok** to complete the transaction.

FAQ

1. Can I edit an Ongoing Transaction Blackout?

Only the End time and End Date of the ongoing blackout can be edited, that too only if it is greater than the current system date and time.

2. Can I edit scheduled Transaction Blackout?

Yes. System Administrator has more flexibility in editing a scheduled transaction blackout.

3. Can I delete an ongoing Transaction blackout?

Yes, ongoing transaction blackout can be deleted. Deleting ongoing blackout will stop the blackout and the transaction will be available to the users post approved by necessary levels of approvals.

4. Any notification will be sent to the users about the planned blackout?

Administrator can send a notification to the users using the mailers feature available.

5. What happens when user tries to access the transaction which is blacked out?

A message is shown on the screen informing about transaction blackout.

50. Working Window

A transaction working window is the period in a day, when a transaction can be initiated, approved and processed. This is essentially like business hours, for a transaction. It is a time window within which electronic payments, such as domestic transfers, international transfers etc., must be submitted for an entry in the system so that the transaction is processed with same value date.

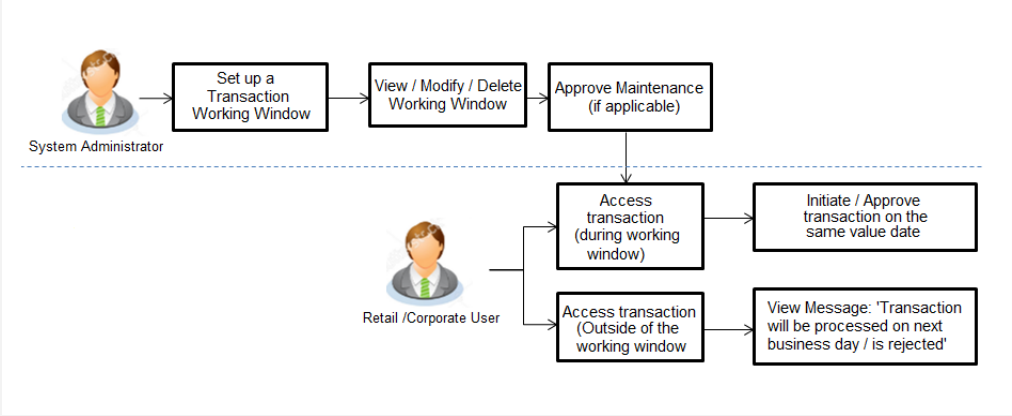
A working window is maintained, by the System Administrator for each transaction for which the value date is applicable for processing. In order to enable such transactions on channel, it is mandatory to define the working window for all the days of a week as day 0 maintenance. By doing this maintenance, user defines the channel working window for each day of the week for a specific transaction. Further, administrator can also define the processing pattern if the transaction is initiated by customers after the window is closed. Transactions, that are initiated or approved outside of the working window, are either processed on the next value date or rejected. Transaction working window can also be maintained for specific date which will be considered as exceptional working window, e.g. maintenance for specific public holiday. Working window set for an exception, overrides the normal working window.

Administrator can set up two different weekly and exceptional working windows for a specific transaction for different user types (Retail and Corporate User).

Pre-Requisites

- Transaction access is provided to System Administrator
- Approval rule set up for System Administrator to perform the actions
- Enable only those transactions for which the working window maintenance is applicable

Workflow



Features Supported In Application

The following options are available as part of this maintenance:

- Create a Transaction Working Window and an Exception for a particular date for all seven days
- Search and View Transaction working windows and Exceptions already maintained
- Delete or Edit transaction working windows / Exceptions maintained.

How to reach here:

System/ Bank Administrator Dashboard > Controls and Monitoring > Working Window
OR
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Controls and Monitoring > Working Window

50.1 Transaction Working Window - Search

This function allows the System Administrator to search the working windows which are already maintained. The search is available on the basis of specific date, transaction and user type.

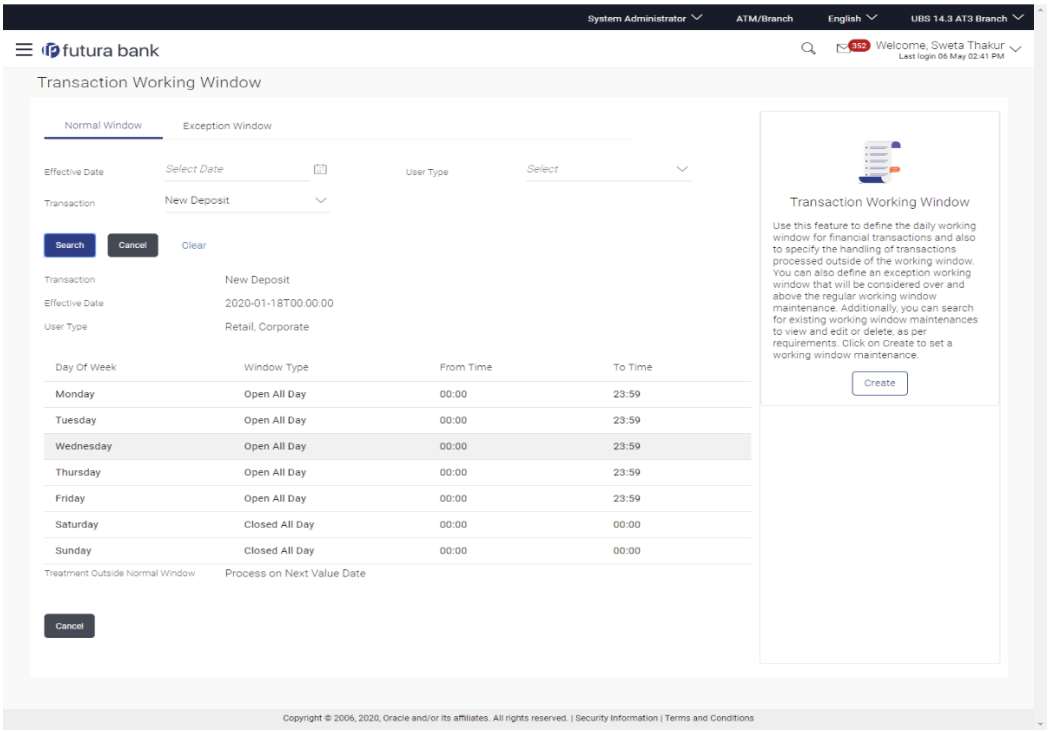
The screen is broadly divided into:

- Normal Window
- Exception Window

To search the working windows:

1. Select the working window.
2. If you select **Normal Window** tab,
   a. Enter the search criteria like **Transaction**, **Effective Date,** or **User Type**.
   b. Click **Search**, displays results based on search criteria.
      OR
      Click **Clear** to clear the search parameters.
      OR
      Click **Cancel** to cancel the transaction.

Search Normal Window



Field Description

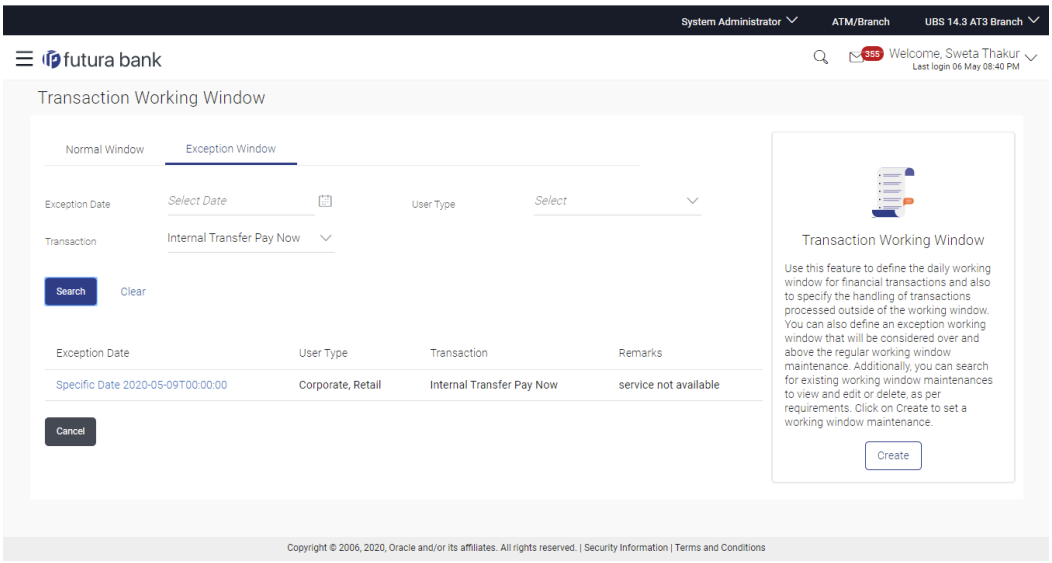
Field Name	Description
Normal Window	
Effective Date	Effective date of working window.
Transaction	The specific financial transaction, for which a working window is maintained.
User Type	The type of user for whom the transaction working window is being maintained. The user types could be: • Corporate User • Retail User
Search Result	
Day of Week	Day of week for which the transaction working window is applicable.

Field Name	Description
Window Type	Type of working window for the transaction. The type can be: • Limited Time • Open All Day • Closed All Day
From Time	Start time of transaction working window. This field is enabled if you select **Limited Time** from the **Window Type** field.
To Time	End time of transaction working window. This field is enabled if you select **Limited Time** from the **Window Type** field.
Other Details	
Treatment Outside Normal Window	Indicates the treatment outside normal window: The options are: • Process on Next Value Date • Reject Transaction

3. View the working window - Current Working Window and Future working window (if any), with the effective date. This is split day wise. Go through the working window time for each day and also how processing is set-up, outside the working window.
4. Click **Edit** to edit the maintenance.
   OR
   Click **Delete** to delete the maintenance.

If you select **Exception Window** tab,

Search Exception Window



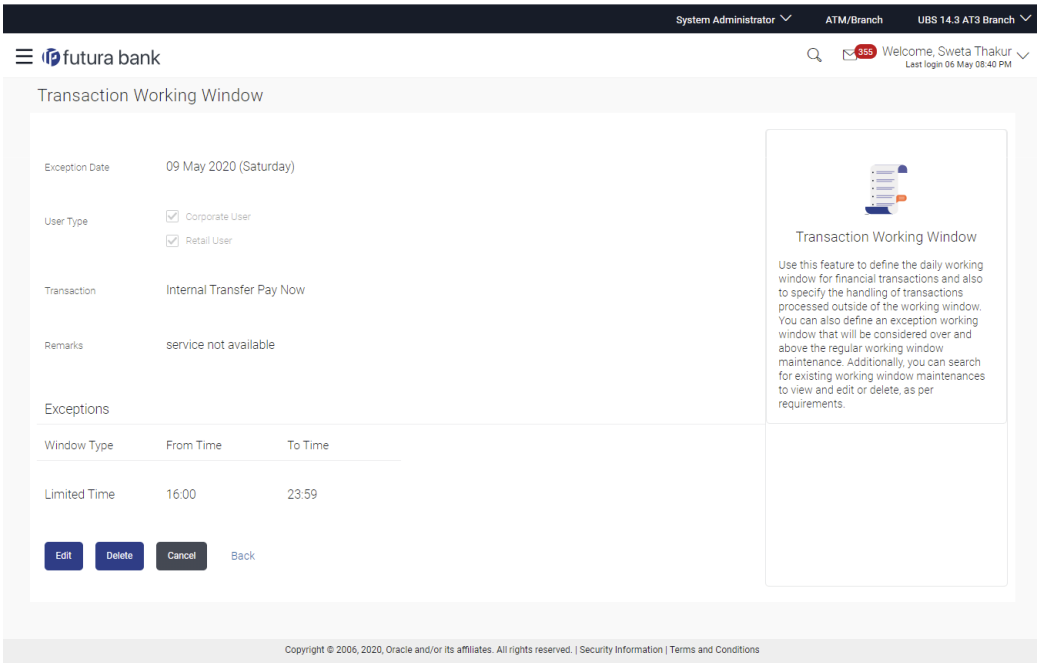
Field Description

Field Name	Description
Exception Window	
Exception Date	Exception date for which the transaction is allowed during the specific date or date range. The exception date could be: • Specific Date: Transaction allowed for a specific date. • Date Range: Transaction allowed during a specified period.
User Type	Type of user, whether the transaction exception is applicable for a retail or corporate user.
Transaction	The specific financial transaction, for which a working window is maintained.
Remarks	Reason for exception.
User Type	Type of user, whether the transaction exception is applicable for a retail or corporate user.
Exceptions	

Field Name	Description
Date and Day	Day and date for which the exception is applicable.
Window Type	Transaction exception applicable window. Window types: • Limited Time: Transaction is applicable for a limited time. • Open all Day: Transaction can be done for the entire day. • Close all Day: Transaction is closed for the whole day.
Time Range	Transactions are open during the specific time. This field is enabled, if you select **Limited Time**, option from the **Window Type** list.

5. Click the **Exception Date** field to launch the **Detailed View** screen.

Search Exception Window- Detailed View



Field Description

Field Name	Description
Exception Date	Exception date for which the transaction is allowed during the specific date or date range.

Field Name	Description
	The exception date could be: • Specific Date: Transaction allowed for a specific date. • Date Range: Transaction allowed during a specified period.
User Type	Type of user, whether the transaction exception is applicable for a retail or corporate user.
Transaction	The specific financial transaction, for which a working window is maintained.
Remarks	Reason for exception.
Exceptions	
Window Type	Type of working window for the exception. Window types: • Limited Time: Transaction is enabled, for the set limited time – the business hours of the transaction • Open all Day: Transaction is enabled, for the entire day. • Close all Day: Transaction is disabled, for the whole day.
Time Range	Business hours of the transaction. This field is enabled, if you select **Limited Time**, option from the **Window Type** list.

6. Click **Edit** to edit the maintenance.
   OR
   Click **Delete** to delete the maintenance.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.

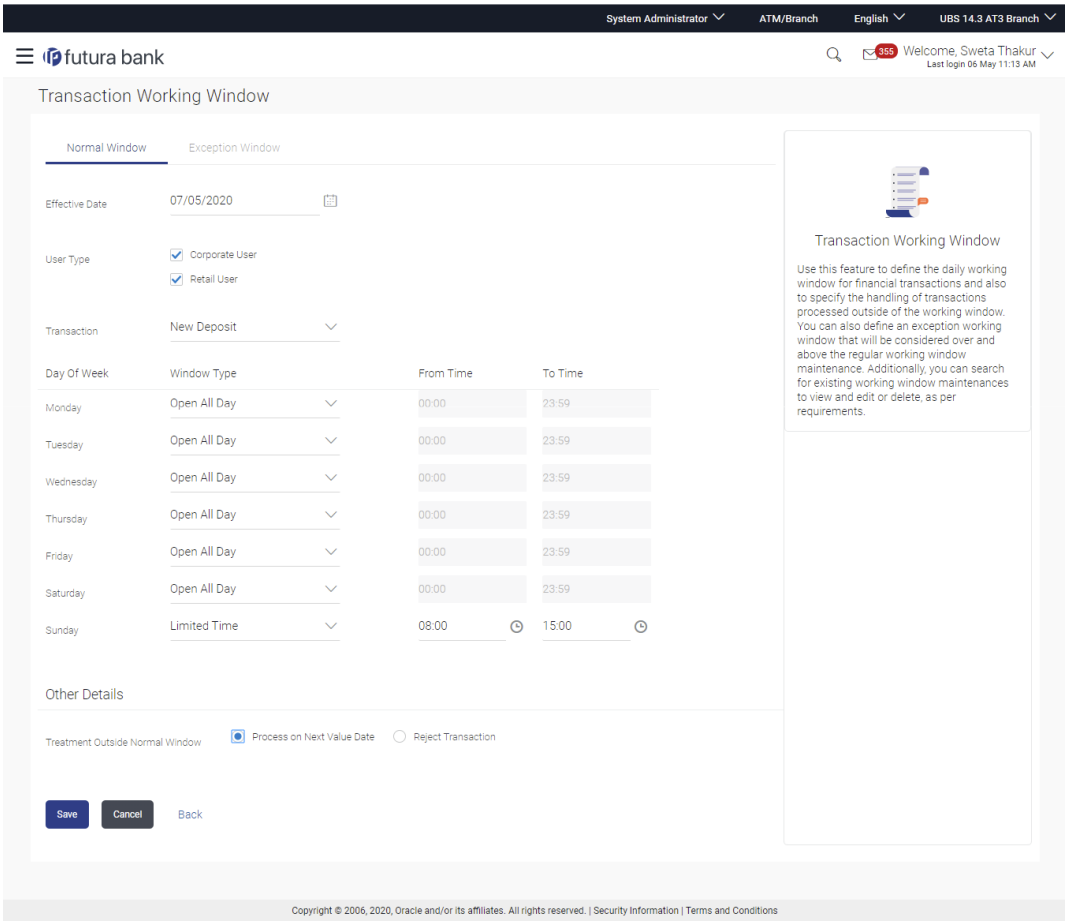
50.2 Transaction Working Window - Create

System Administrator can create new transaction working window maintenance for the selected transaction. Working window can be set as 'Normal' working window (for all days of the week) and 'Exception Window'.

To create normal window:

1. Select the working window.
2. If you select **Normal Window** tab,
   a. Click **Create**.

Create Working Window



Field Description

Field Name	Description
Effective Date	Effective date of working window.
User Type	The type of user for whom the transaction working window is being maintained. The user types could be: • Corporate User • Retail User
Transaction	The specific financial transaction, for which a working window is maintained.

Field Name	Description
Day of Week	Day of week for which the transaction working window is applicable.
Window Type	Type of working window for the transaction. The type can be: • Limited Time • Open All Day • Closed All Day
From Time	Start time of transaction working window. This field is enabled if you select **Limited Time** from the **Window Type** field.
To Time	End time of transaction working window. This field is enabled if you select **Limited Time** from the **Window Type** field.
Other Details	
Treatment Outside Normal Window	Indicates the treatment outside normal window: The options are: • Process on Next Value Date • Reject Transaction

b. From the **Effective Date** list, select the start date of the transaction working window.

c. From the **Window Type**, select the appropriate option.

d. If you select the **Window Type** as **Limited Time**, from the **From Time** / **To Time** list select the start and end time of the transaction working window.

e. In the **Other Details** section, from the **Treatment Outside Normal Window** field, select the appropriate option.

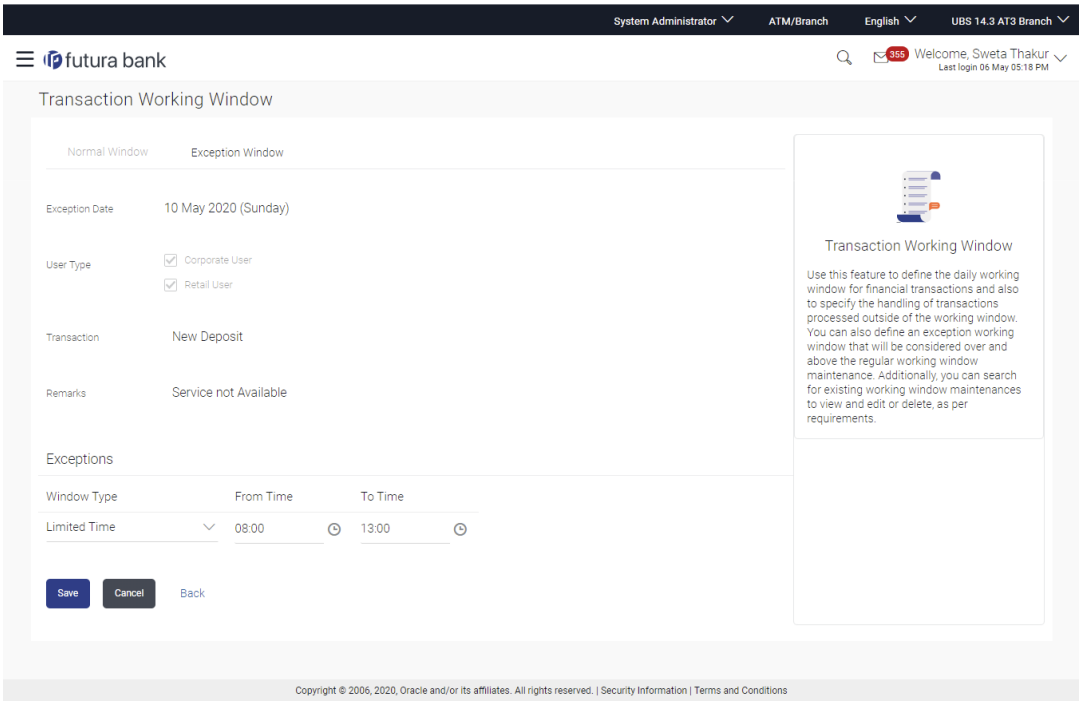
3. Click **Save** to create the transaction working window.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.
4. The **Review** screen is displayed. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to modify details if any.
   OR
   Click **Cancel** to cancel the transaction.

5. The success message is displayed along with the transaction reference number. Click **OK** to complete the transaction.

To create Exception window:

1. Select the working window.
2. If you select **Exception Window** tab,
   a. Click **Create.**

Create Exception Window



Field Description

Field Name	Description
Exception Date	Exception date or date range, when processing for a transaction, overrides that set in the normal transaction working window. The exception date could be: • Specific Date: Exception for a single day • Date Range: Exception for a date range
User Type	Type of user, whether the transaction exception is applicable for a retail or corporate user.

Field Name	Description
Transaction	The specific financial transaction, for which an exceptional working window is maintained.
Remarks	Reason for exception for e.g. a national holiday.
Exceptions	Type of working window for the transaction. Window types: • Limited Time • Open all Day • Close all Day
Window Type	Type of working window for the exception. Window types: • Limited Time: Transaction is applicable for a limited time. • Open all Day: Transaction can be done for the entire day. • Close all Day: Transaction is closed for the whole day.
Time Range	Business hours of the transaction. This field is enabled, if you select **Limited Time**, option from the **Window Type** list.

b. From the **Exception Date** list, select the start date of the working window - exception.

c. From the **Window Type**, select the appropriate option.

d. If you select the **Window Type** as **Limited Time**, from the **From Time** / **To Time** list select the start and end time of the working window - exception.

3. Click **Save** to create the transaction working window.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to close the exception creation process.
4. The **Review** screen is displayed. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to modify details if any.
   OR
   Click **Cancel** to cancel the transaction.
5. The success message is displayed along with the transaction reference number. Click **OK** to complete the transaction.

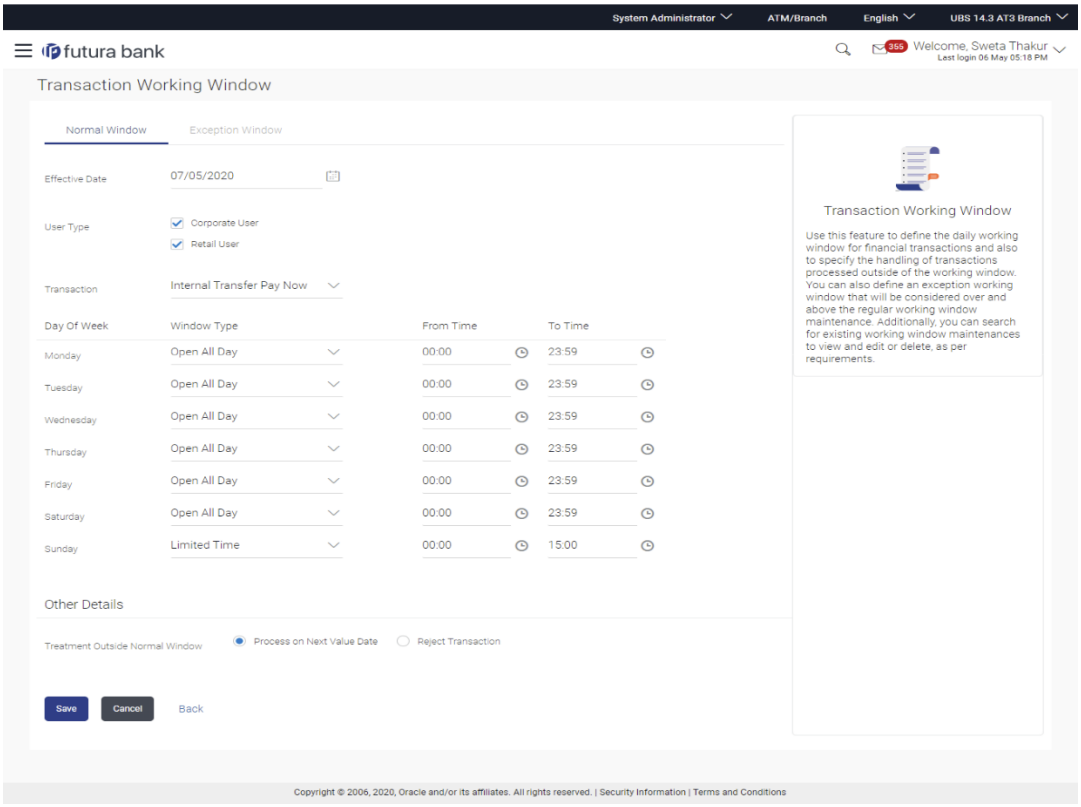
50.3 Transaction Working Window - Edit

System Administrator can modify existing working window maintenance. In case of normal working window, edit is allowed only if the effective date is a future date. In case of exception working window, future window can be edited current exceptional window can also be edited if the set time is less than the actual time.

To modify normal window:

1. Select the working window.
2. If you select **Normal Window** tab,
   a. Enter the search criteria like **Transaction**, **Effective Date,** or **User Type**.
   b. Click **Search**, displays results based on search criteria.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.
   c. Click **Edit** to edit the working window, from the Detailed View page.
   OR
   Click **Delete** to delete the maintenance.

Edit Normal Window



Field Description

Field Name	Description
Effective Date	Effective date of working window.
User Type	The type of user for whom the transaction working window is being maintained. The user types could be: • Corporate User • Retail User
Transaction	The specific financial transaction, for which a working window is maintained.
Window Type	Type of working window for the transaction. The type can be: • Limited Time • Open All Day • Closed All Day
From Time	Start time of transaction working window. This field is enabled if you select **Limited Time** from the **Window Type** field.
To Time	End time of transaction working window. This field is enabled if you select **Limited Time** from the **Window Type** field.
Other Details	
Treatment Outside Normal Window	Indicates the treatment outside normal window: The options are: • Process on Next Value Date • Reject Transaction

d. View the effective date, from when the modified maintenance will be effective. Modify if required.

e. The user can view the days of the week – from Monday through Sunday with a drop-down of three values against each day(Open all Day, Closed all day, Limited Time)

Note: For open all day and closed all day options, system defaults from and to time values of– 00:00 and 23:59 hours, for the former and 00:00 hours, for the latter. For the limited time option, specify from and to time, to define the transaction working window.

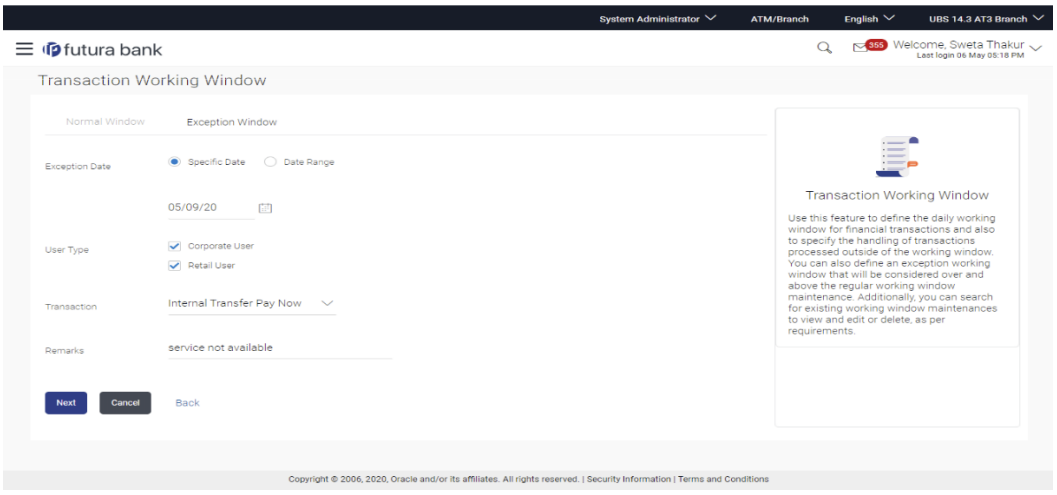
f. View the preferred processing, when transaction is initiated or approved outside of the working window.
Either Process on Next Value Date or Reject Transaction Modify if required.

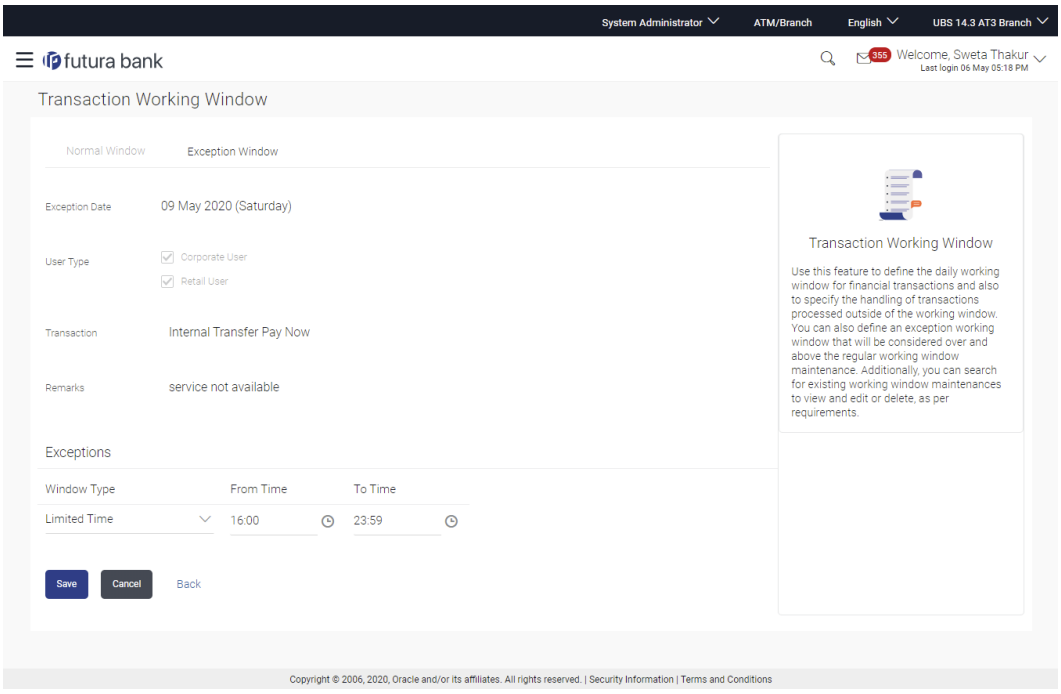
3. Click **Save** to create the transaction working window.
OR
Click **Cancel** to close the exception creation process.
OR
Click **Back** to navigate to the previous screen.
4. The **Review** screen is displayed. Verify the details, and click **Confirm**.
OR
Click **Edit** to modify details if any.
OR
Click **Cancel** to cancel the transaction.
5. The success message is displayed along with the transaction reference number. Click **OK** to complete the transaction.

To modify exception window:

1. Select the working window.
2. If you select **Exception Window** tab,
   a. Enter the search criteria like **Transaction**, **Effective Date,** or **User Type**.
   b. Click **Search**, displays results based on search criteria.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.
   c. Click **Edit** to edit the working window - exception, from the Detailed View page.
   OR
   Click **Delete** to delete the maintenance.

Edit Exception Window





Field Description

Field Name	Description
Exception Date	Exception date or date range, when processing for a transaction, overrides that set in the normal transaction working window. The exception date could be: • Specific Date: Exception for a single day • Date Range: Exception for a date range
User Type	Type of user, whether the transaction exception is applicable for a retail or corporate user.
Transaction	The specific transaction, for which exception is being maintained.
Remarks	Reason for exception for e.g. a national holiday.
Exceptions	

Field Name	Description
Window Type	Type of working window for the exception. Window types: • Limited Time: Transaction is applicable for a limited time. • Open all Day: Transaction can be done for the entire day. • Close all Day: Transaction is closed for the whole day.
Time Range	Business hours of the transaction. This field is enabled, if you select **Limited Time**, option from the **Window Type** list.

3. Update the required details.
4. Click **Save** to create the transaction working window.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to close the exception creation process.
5. The **Review** screen is displayed. Verify the details, and click **Confirm**.
   OR
   Click **Edit** to modify details if any.
   OR
   Click **Cancel** to cancel the transaction.
6. The success message is displayed along with the transaction reference number. Click **OK** to complete the transaction.

50.4 Transaction Working Window - Delete

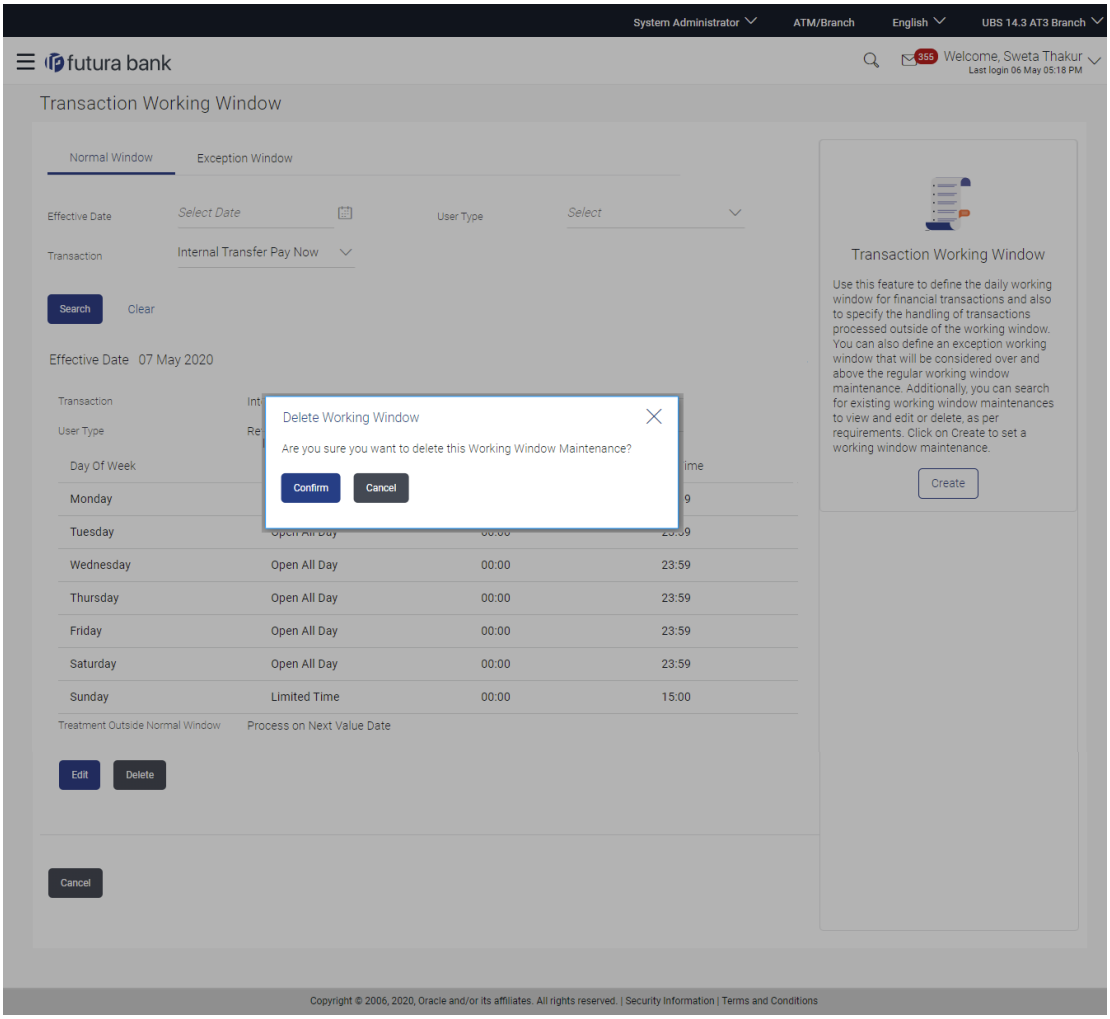
System Administrator can delete existing working window maintenance. User is allowed to delete future dated maintenances.

To delete normal window:

1. Select the working window.
2. If you select **Normal Window** tab,
   a. Enter the search criteria like **Transaction**, **Effective Date,** or **User Type**.
   b. Click **Search**, displays results based on search criteria.
      OR
      Click **Clear** to clear the search parameters.
      OR
      Click **Cancel** to cancel the transaction.

c. Click **Edit** to edit the working window, from the Detailed View page.
OR
Click **Delete** to delete the working window, from the Detailed View page.

Delete Normal Window

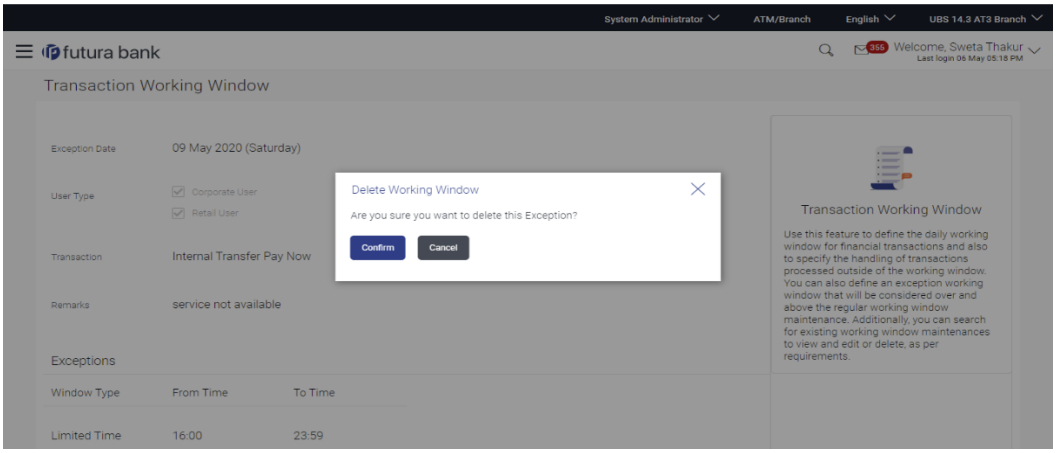


To delete exception window:

1. Select the working window.
2. If you select **exception Window** tab,
   a. Enter the search criteria like **Transaction**, **Effective Date,** or **User Type**.
   b. Click **Search**, displays results based on search criteria.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.

c. Click **Edit** to edit the working window, from the Detailed View page.
OR
Click **Delete** to delete the working window - exception, from the Detailed View page.

Delete Exception Window



- The user can delete a future transaction working window or an exception with an effective date in the future.
- Navigate to the particular working window or the exception and click on Delete.
- The system displays a pop-up message with Confirm and Cancel buttons. On confirming deletion, system displays a transaction successful message, provides a reference number and the status of the maintenance (e.g. pending approval)
- If the user chooses to cancel the transaction, he's directed to the admin dashboard

FAQ

1. **Can I set the transaction working window from the current date?**

   No, you cannot set the transaction working window date from current date. You can set that from future date.

2. **If a particular day, have both a normal working window set, and an exception – which will take precedence?**

   Working window set for an exception, overrides the normal working window set.

3. **If the normal working window for a transaction is set for Open all Day and an Exception is set as Closed all Day, will I be able to initiate transaction, on that day?**

   No, I will not be able to initiate the transaction on that day. The transaction will either have the next working day's value date or be rejected.

4. **Can I delete or edit current applicable normal working window?**

   No, current applicable normal working window cannot be edited or deleted. User can add a new window with future effective date.

5. **Can I set 'behavior of transaction outside working window' for exceptional days?**

   No, behavior of transaction outside working window for exceptional date maintenance will remain same as normal window maintenance.

51. Audit Log

Audit log is set of records that provide information about operations performed in the application and details of the user who has performed it along with date and time when it was performed.

Audit logs are useful both for maintaining security and for auditing any disputed transaction. As part of this function, the bank administrator and/or system administrator can view details about the transactions and maintenances performed by different user(s) in the system.

The administrator can search records by providing specific search parameters and system will display matching records for the search criteria. Maintenances created/edited/deleted/inquired by bank administrator can be audited through this function by the system administrator. Maintenances created/edited/deleted/inquired by corporate administrator can be audited through this function by the bank as well as system administrator.

Transactions carried out by corporate users can be audited if required by the Corporate or Bank administrator and also by system administrator.

Prerequisites

- Transaction access is provided to System and Bank administrator.
- Transactions are available under respective users to check audit log.

How to reach here:

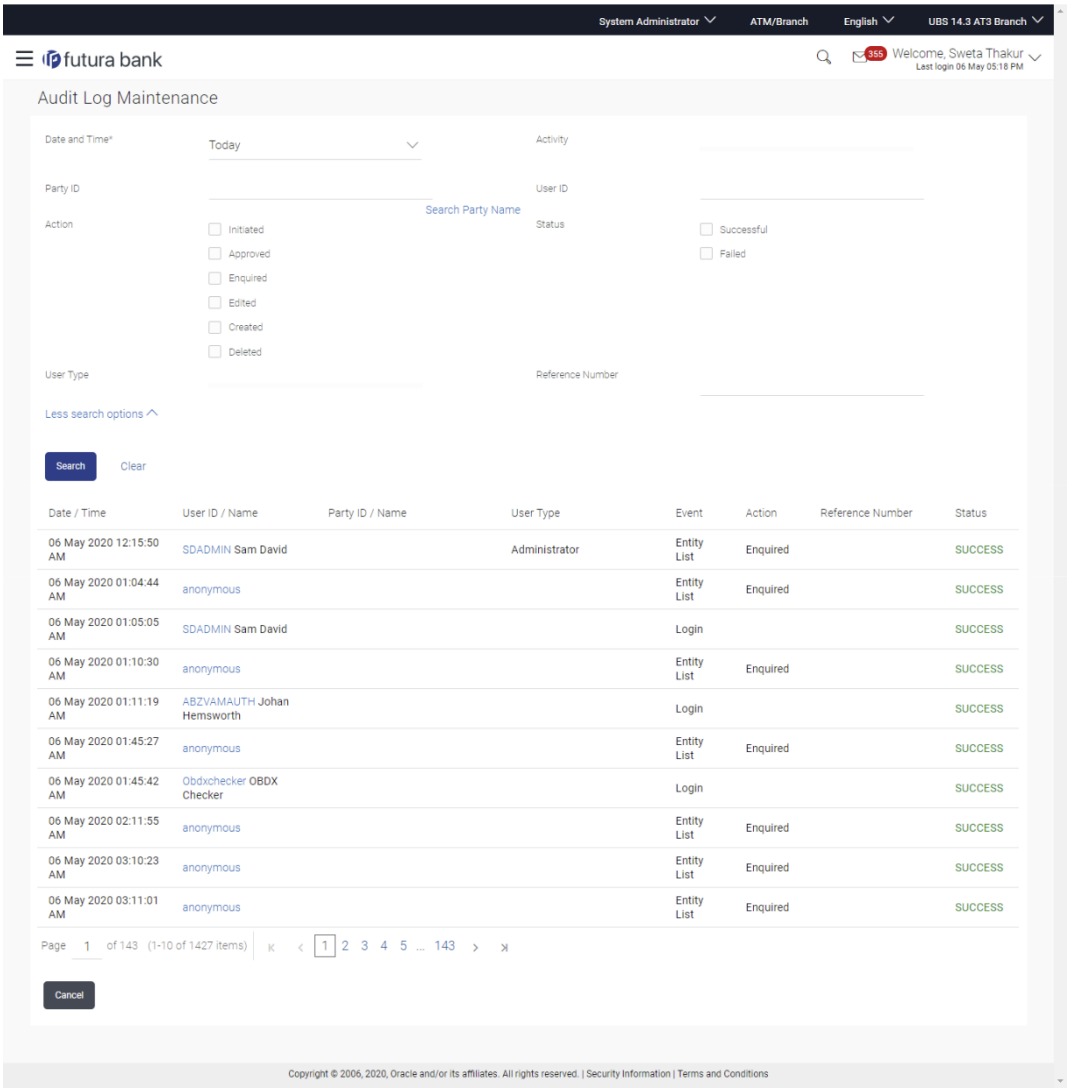
System/ Bank Administrator Dashboard >Controls and Monitoring> Audit Log
OR
System/ Bank Administrator Dashboard > Toggle menu > Menu > Controls & Monitoring > Audit Log

51.1 Search Audit Details

To view audit log:

1. From the **Date and Time** list, select the period for which you want to view the audit log.
2. Enter required search criteria. Click **Search**.
   Audit log appears based on the entered search parameters.
   OR
   Click **Clear** to reset the details.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.

Audit Log- Search



Field Description

Field Name	Description
Date and Time	The date and time from which audit log is to be generated. The options are: • Today • Yesterday • Last 3 days • Date Range

Field Name	Description
From	Start date and time of the request processing. This field appears if you select **Date Range** option from the **Date and Time** list.
To	End date and time of the request processing. This field appears if you select **Date Range** option from the **Date and Time** list.
Activity	Select specific transaction or maintenance from the list.
Party ID	Party ID of the logged in user for which audit details are logged.
Search Party Name	Click on the **Search Party Name** link, the pop up window appears. User can search the Party ID by entering keywords of party name. Click **Search** to search the party ID. The search result appears based on party name, select appropriate party. OR Click **Clear** to reset the search parameters.
User ID	User ID for which the audit details are logged.
Action	Type of action. The options are: • **Initiated**: To be selected if only initiated transactions are to be searched • **Approved**: To be selected if only transactions/maintenances in approved state are to be searched. • **Enquired**: To be selected if only maintenances which were enquired are to be searched • **Edited**: To be selected if only maintenances which were edited are to be searched • **Created**: To be selected if only maintenances which were created are to be searched • **Deleted**: To be selected if only maintenances which were deleted
Status	Status of the transaction. The options are: • Success • Failed

Field Name	Description
User Type	To be selected if the search is to be based on the user type. Multiple user types can be selected. Following are user types. • Retail User • Corporate User • Administrator
Reference Number	Search based on Reference number of the transaction.
Search Result	
Date / Time	The date and time of the activity i.e. transaction/maintenance.
User ID/ Name	User ID and Name of the user who performed the transaction or carried out the maintenance. Click on the hyperlink available on the User ID to view the Request/response details of the transaction/maintenance in json format.
Party ID/ Name	Party ID and Party name for which the maintenance or transaction was carried out.
User Type	User type of the user who performed an activity i.e. maintenance/transaction.
Event	Name of transaction/maintenance for which audit details of transaction are logged.
Action	Name of transaction action. • Enquired • Initiated • Created • Edited • Deleted • Approved
Reference Number	Reference number of the transaction/maintenance.

Field Name	Description
Status	Status of the transaction. The options are: • Success • Failed

FAQ

1. **Do I need to enter all the parameters to search?**

   No. You need to enter at least the date and time criteria to proceed with audit search. Rest of the search parameters are optional and can be entered if the search results are to be narrowed down.

2. **I do not remember the party ID for input, can I search a party if I need to view audit details for a specific party?**

   Yes. You can search a party by clicking ‘Search Party’ and searching the party by entering the party name.

3. **As part of input search criterion/parameters, in the action field there are certain options disabled. Is there a specific reason?**

   If you select any maintenance in the activity field, ‘Initiated’ as an action will not be available. If you select any transaction in the activity field, ‘Created’, ‘Edited’ or ‘Deleted’ as actions will not be available.

52. File Upload

File Uploads facilitates processing of multiple transactions through a single file. This is a faster way of processing transactions than entering single screen transactions. Salary payments, fund transfers, vendor payments are few examples of financial transactions that can be supported through file upload. A non-financial transaction to facilitate upload of multiple payee details, at a single instance, is also possible through file upload.

OBDX has made File Upload functionality available for both Corporate and Bank Users.

Some of the file uploads available for Corporate User are:

- Internal payments (within the bank)
- Domestic payments (within the country)
- International payments (cross border)
- Mixed payments
- Create Payees / Beneficiaries
- Create Virtual Accounts, Structure & Identifiers

File upload available for Bank User

- Bill Presentment

Oracle Banking Digital Experience File Upload module enables banks to process files of payments according to agreed operational and business rules and save time. File Uploads facility is simple to use, has daily transaction limits and comes with the security of dual / multi signatory approvals.

- File Upload Set up: Enables the administrator to create file identifiers, and map users to file identifiers.
- File Upload Servicing: Enables the corporate user to upload, view and approve files, (files that the user has access to).

File Upload Set up

File Upload set up covers the maintenance part of file upload and is performed by an administrator user. As a part of the initial set-up, the administrator user -

- Creates a File Identifier for a File Template using the ‘File Identifier’ option
- Maps a File Identifier to a user using the ‘User File Identifier Mapping’ option

52.1 File Identifier Maintenance

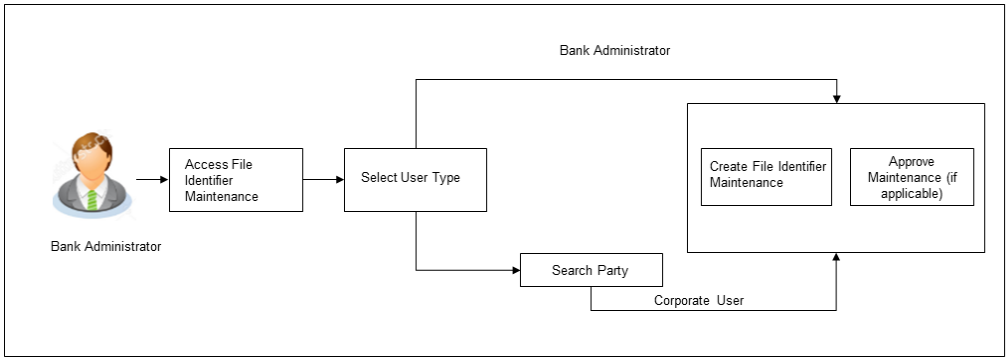
Bank Administrator can create file identifiers (FI) to upload files for corporate as well as bank administrator users. This enables the corporate users and bank administrators to process file uploads. A File Identifier is always mapped to a specific file template. It permits configuration of party preferences like approval type (file level / record level) for a particular type of file.

Prerequisites

- Transaction access is provided to Bank Administrator
- User Creation
- Set up Party Account access (for corporate file upload)
- Set up Transaction Account access (for corporate file upload)
- Set up Approval Rules (for corporate file upload)

Features Supported In Application

- Search File Identifier
- Create File Identifier
- Edit File Identifier



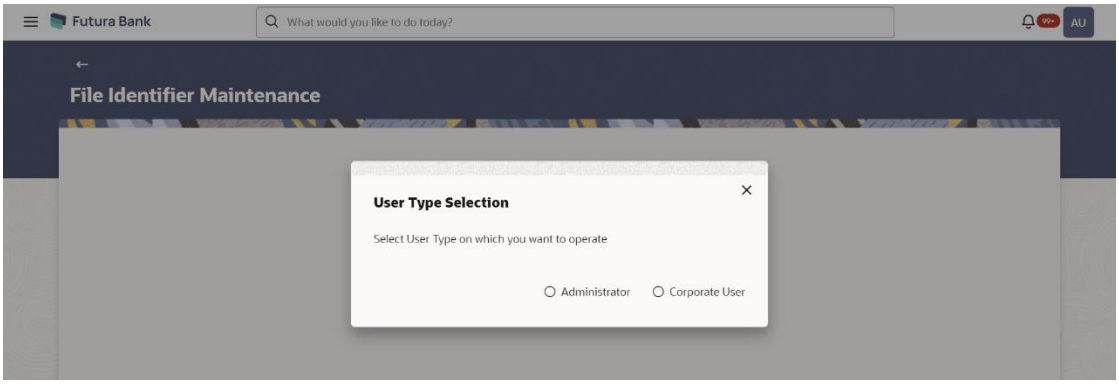
How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > File Upload > File Identifier Maintenance
OR
Bank Administrator Dashboard > Quick Links > File Upload > File Identifier Maintenance
OR
Search Bar > File Upload - File Identifier Maintenance

52.1.1 File Identifier Maintenance – User Type Selection

Bank Administrator logs into the system and navigates to the File Identifier Maintenance screen. On accessing the 'File Identifier Maintenance' menu, bank administrator has to select the user type.

File Identifier Maintenance – User Type Selection



1. Click **Administrator** to access the file identifier for bank administrator users. The File Identifier Maintenance screen appears.
2. Click **Corporate User** to access the file identifier of corporate users. The File Identifier Maintenance screen appears.

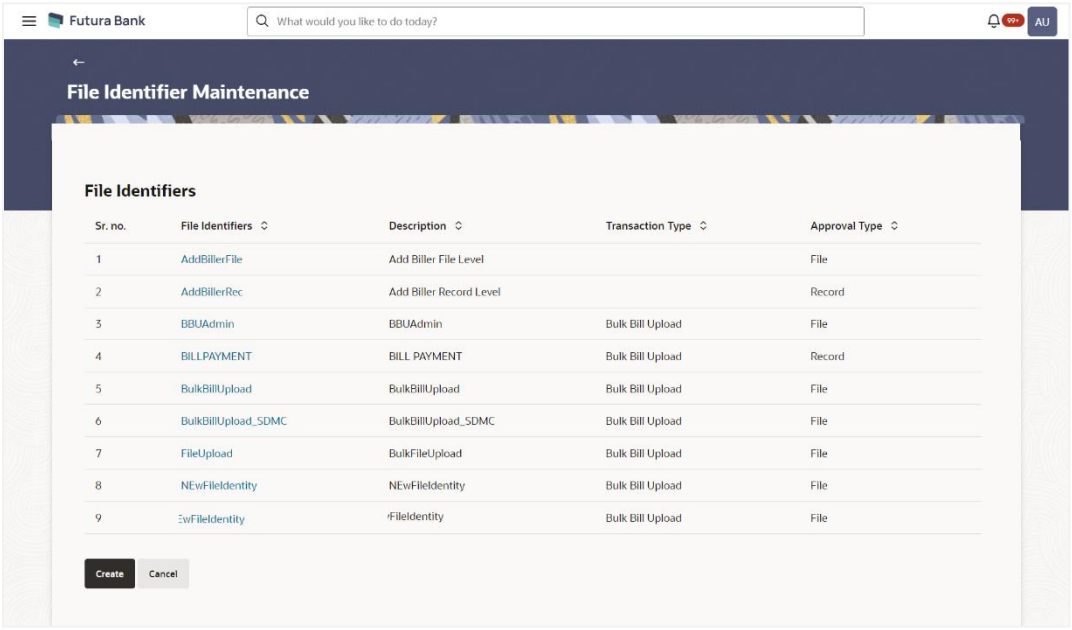
52.1.2 File Identifier Maintenance - Administrator User – Summary

For the bank administrators the only file upload available is for the uploading of Bill Presentment file. Once the logged in user navigates to File Identifier Maintenance (Administrator User) screen, user can view the record details of the File Identifiers already created.

To search and view the file identifiers:

1. Navigate to the **File Identifier Maintenance** screen. The **File Identifier** - summary screen appears.

File Identifier - Summary

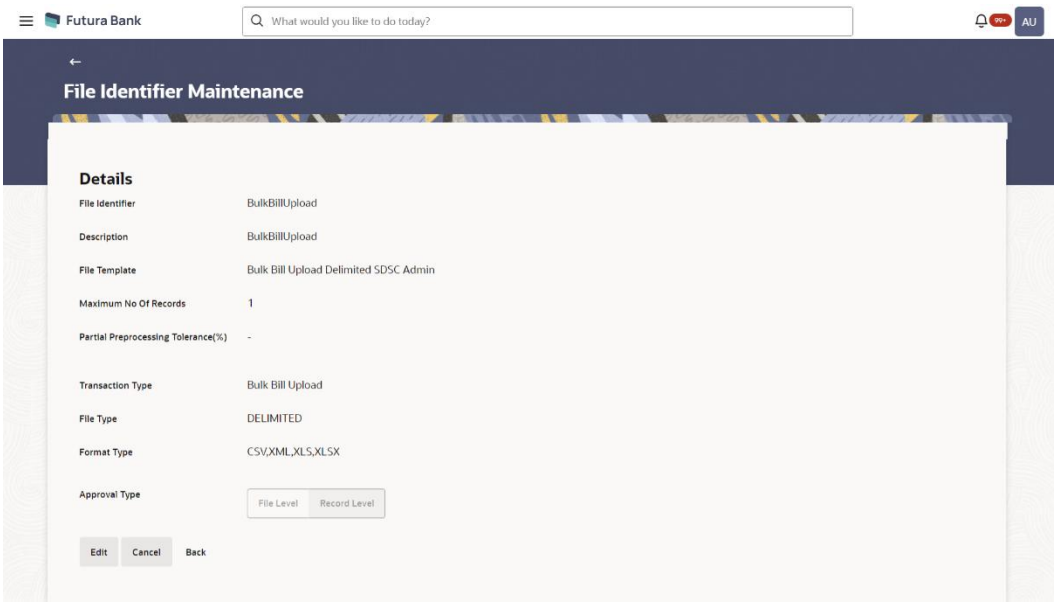


Field Description

Field Name	Description
File Identifiers	
Sr. No.	Serial number of the record.
File Identifiers	Unique code/ name assigned as per party preferences for handling of payment files.
Description	File name / code description corresponding to the file upload code.
Transaction Type	Type of transaction: The Transaction types could be: • Bulk Bill Upload
Approval Type	The approval type is at file level or record level.

2. Click the **File Identifier** link against the record, for which you want to view the details.
   The **File Identifier Maintenance- View** screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Create** to create a new file identifier.

File Identifier Maintenance - View



Field Description

Field Name	Description
Details	
File Identifier	Unique code/ name assigned for handling of payment files.
Description	File name / code description corresponding to the file upload code.
File Template	Predefined file templates. Following file templates are available: • Bulk Bill Upload
Maximum No of Records	Maximum number of records permissible in the uploaded file.
Partial Processing Tolerance (%)	The partial processing tolerance for a file (in percentage terms). Suppose, the user sets this value at 60% - this implies that if 60% or more, of the records in a file clear the validation stage, then the file can go for further processing. If less than 60% of the records in a file clear the validation stage, then the file is rejected.
Transaction Type	Type of transaction: The Transaction type can be: • Bulk Bill Upload
File Type	The file type - delimited or fixed length.

Field Name	Description
Format Type	The format in which file is uploaded. The format could be .CSV, .XLS, .XLSX.
Approval Type	The approval type is at file level or record level. • **File Level** - The approver accepts or rejects the entire file, and all records are either processed or rejected en-masse. • **Record Level**- The approver accepts some records, and rejects others. Payments are processed only for approved records.

3. Click **Edit** to modify the file identifier.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.

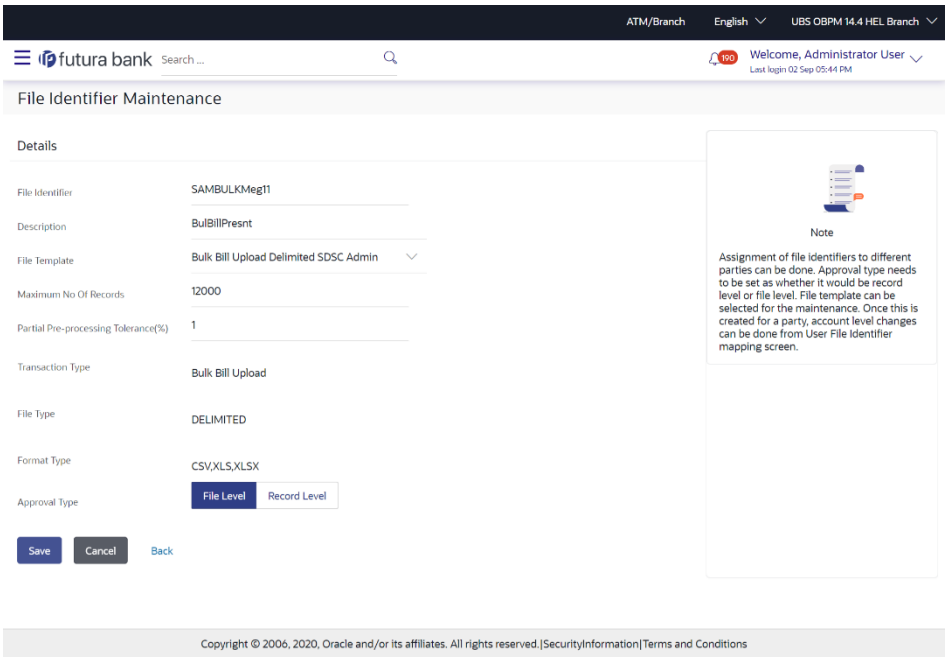
52.1.3 File Identifier Maintenance - Administrator User - Create

Using this option the administrator user can create a new file identifier.

To create a file identifier:

1. In the **File Identifier Maintenance** screen, click **Create**. The **File Identifier Maintenance - Create** screen appears.

File Identifier Maintenance - Create



Field Description

Field Name	Description
Details	
File Identifier	Unique code or name assigned to the uploaded file.
Description	Descriptions corresponding to the file identifier.
File Template	Predefined file templates. Following file templates are available: • Bulk Bill Upload
Maximum No of Records	Maximum number of records permissible in the uploaded file.
Partial Processing Tolerance (%)	The partial processing tolerance for a file (in percentage terms). Suppose, the user sets this value at 60% - this implies that if 60% or more, of the records in a file clear the Validation stage, then the file can go for further processing. If less than 60% of the records in a file clear the validation stage, then the file is rejected. This field is enabled if approval is ‘Record Type’.

Field Name	Description
Transaction Type	Type of transaction: The Transaction type could be: • Bulk Bill Upload
File Type	The file type – delimited or fixed length.
Format Type	The format in which file is uploaded. The format could be CSV, XLS, XLSX.
Approval Type	The approval type is at file level or record level. • File Level - The approver accepts or rejects the entire file, and all records are either processed or rejected en-masse. • Record Level- The approver accepts some records, and rejects others. Payments are processed only for approved records. Note: Approval Type cannot be modified once it is created.

2. In the **File Identifier** field, enter the code of the file to be maintained for upload.
3. In the **Description** field, enter the file description corresponding to the file code.
4. From the **File Template** list, select the file template.
5. Select the appropriate **Approval Type**.
6. Click **Save**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.
7. The **File Identifier Maintenance - Review** screen appears. Verify the details and click **Confirm**.
   form.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.
8. The success message appears along with the transaction reference number and status. Click **OK** to complete the transaction and navigate back to 'Dashboard'.

52.1.4 File Identifier Maintenance - Administrator User – Edit

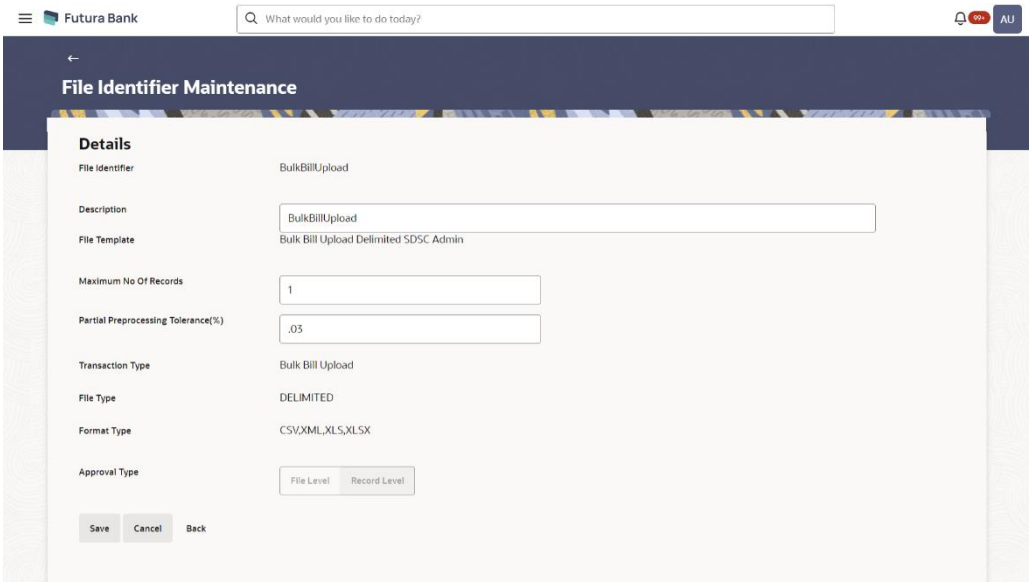
Using this option the administrator can edit and update a file identifier.

To edit file identifier:

1. In the **File Identifier Maintenance** screen, click the **File Identifier** link against the record, which you want to modify.
   The **File Identifier Maintenance- View** screen appears.

2. Click **Edit** to edit the file identifier.
   The **File Identifier Maintenance - Edit** screen appears.

File Identifier Maintenance - Edit



3. Update the required fields of file identifiers. E.g. Description, Maximum Number of Records, and Partial Processing Tolerance, Debit Account Number – if required.

Field Name	Description
Description	Descriptions corresponding to the file upload code.
Maximum No of Records	Maximum number of records permissible in the uploaded file.
Partial Processing Tolerance (%)	The partial processing tolerance for a file (in percentage terms) Suppose, the user sets this value at 60% - this implies that if 60% or more, of the records in a file clear the Validation stage, then the file can go for further processing. If less than 60% of the records in a file clear the validation stage, then the file is rejected.

4. Click **Save** to save the modified details.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to previous screen.
5. The **File Identifier Maintenance – Edit - Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.

OR
Click **Back** to navigate to previous screen.

6. The success message appears along with the transaction reference number and status. Click **OK** to complete the transaction and navigate back to ‘Dashboard’.

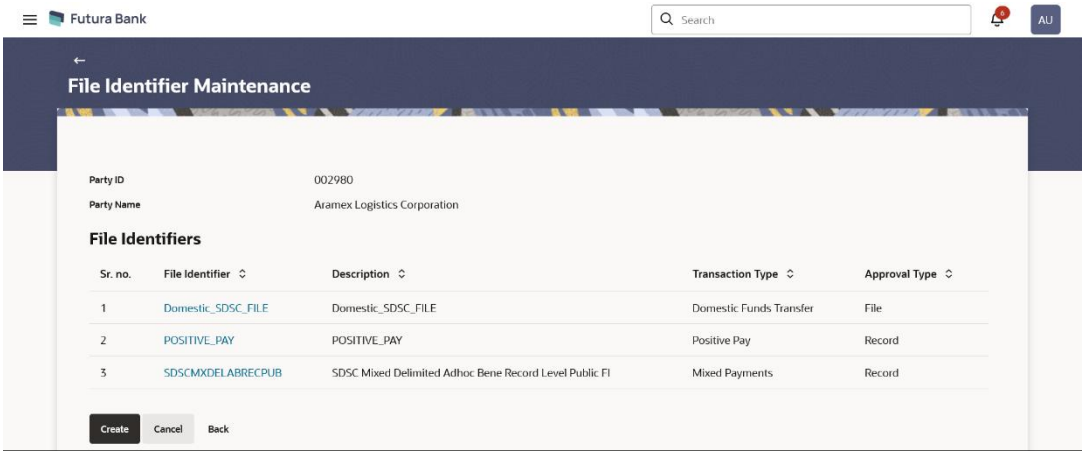
52.1.5 File Identifier Maintenance - Corporate User – Search and View

Once the logged in user navigates to File Identifier Maintenance (for Corporate User) screen, user can search and view the files that are uploaded under a party with the future date with file type as SDSC(Single Debit Single Credit), SDMC (Single Debit Multiple Credit), and MDMC (Multiple Debit Multiple Credit) and view the record details of the File Identifiers already created.

To search and view the file identifiers:

7. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the name of the party.
8. Click **Search**. The **File Identifier Maintenance** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.

File Identifier Maintenance - Search



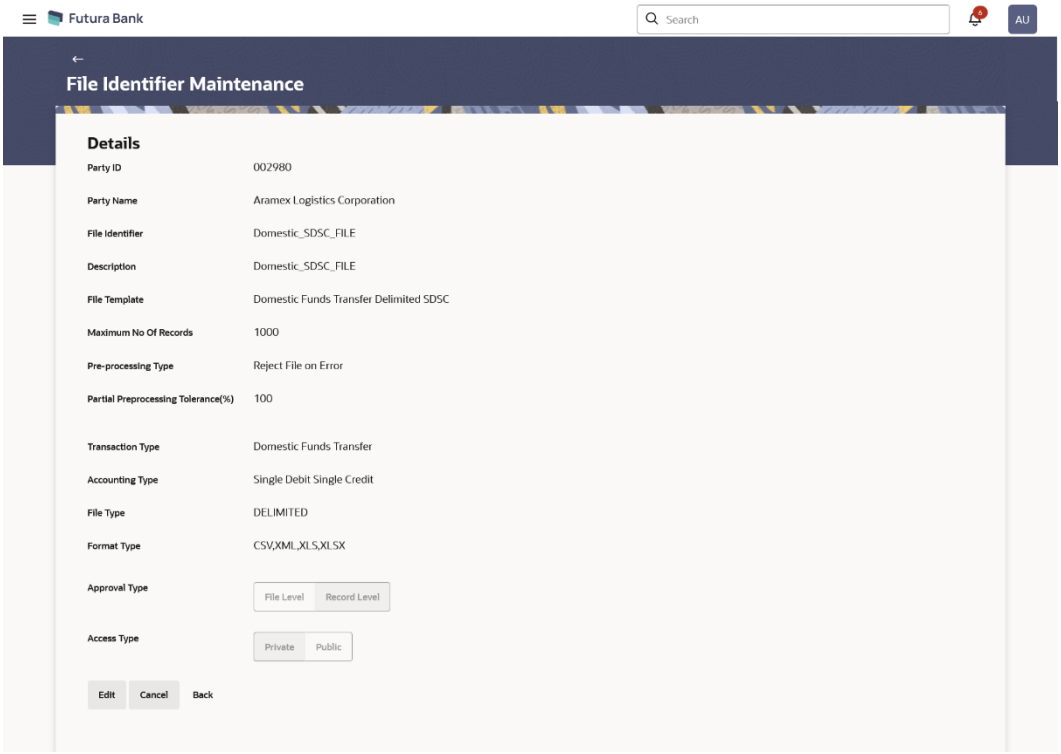
Field Description

Field Name	Description
Party ID	Party ID of the corporate for whom the file identifier is created.
Party Name	Party name corresponding to the party id.
File Identifiers	
Sr. No.	Serial number of the record.
File Identifier	Unique code/ name assigned as per party preferences for handling of payment files.
Description	File name / code description corresponding to the file upload code.

Field Name	Description
Transaction Type	Type of transaction: The Transaction types could be: • Internal Funds Transfer • Domestic Funds Transfer • International Funds Transfer • Mixed Transfer • Internal Payee • Domestic Payee • International Payee • Mixed Payee • Domestic Demand Draft Payee • International Demand Draft Payee • Create Virtual Accounts • Delete Virtual Accounts • Create Virtual Account structure • Create Virtual Identifier • Create Invoice • Bulk Bill Upload
Approval Type	The approval type is at file level or record level.

9. Click the **File Identifier** link against the record, for which you want to view the details.
   The **File Identifier Maintenance- View** screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to go back to previous screen.

File Identifier Maintenance - View



Field Name	Description
Party ID	The party id searched by the bank administrator.
Party Name	Party name corresponding to the party ID.
Details	
File Identifier	Unique code/ name assigned for handling of payment files.
Description	File name / code description corresponding to the file upload code.
File Template	Predefined file templates. Following file templates are available: • Domestic Funds Transfer Delimited SDSC • Domestic Funds Transfer Fixed SDSC • Domestic Funds Transfer Delimited MDMC • Domestic Funds Transfer Fixed MDMC • Domestic Funds Transfer Delimited SDMC

Field Name	Description
	• Domestic Funds Transfer Fixed SDMC • Domestic Funds Transfer Delimited SDSC with Account ID defined at File Identifier level • Internal and Domestic Funds Transfer Delimited SDMC • Internal and Domestic Funds Transfer Fixed SDMC • Internal Funds Transfer Delimited SDSC • Internal Funds Transfer Fixed SDSC • Internal Funds Transfer Delimited MDMC • Internal Funds Transfer Fixed MDMC • Internal Funds Transfer Delimited SDMC • Internal Funds Transfer Fixed SDMC • Internal Funds Transfer Delimited SDMC with Account ID defined at File Identifier level • Internal Funds Transfer Delimited SDSC with Account ID defined at File Identifier level • International Funds Transfer Delimited SDSC • International Funds Transfer Fixed SDSC • International Funds Transfer Delimited MDMC • International Funds Transfer Fixed MDMC • International Funds Transfer Delimited SDMC • International Funds Transfer Fixed SDMC • Demand Draft Payees • Domestic Payees • Internal payees • International Payees • Mixed Payees • Mixed Payments Delimited MDMC • Mixed Payments Fixed MDMC • Mixed Payments Delimited SDSC • Mixed Payments Fixed SDSC • Create Virtual Accounts • Create Virtual Accounts Structure • Create Virtual Identifier

Field Name	Description
	• Create Invoice • Bulk Bill Upload
Maximum No of Records	Maximum number of records permissible in the uploaded file.
Partial Processing Tolerance (%)	The partial processing tolerance for a file (in percentage terms). Suppose, the user sets this value at 60% - this implies that if 60% or more, of the records in a file clear the validation stage, then the file can go for further processing. If less than 60% of the records in a file clear the validation stage, then the file is rejected.
Debit Account Number	Account number from which amount is to be debited. This field appears for templates having **AcctId defined at FI level.**
Transaction Type	Type of transaction: The Transaction type can be: • Internal Funds Transfer • Domestic Funds Transfer • International Funds Transfer • Mixed Transfer • Internal Payee • Domestic Payee • International Payee • Mixed Payee • Domestic Demand Draft Payee • International Demand Draft Payee • Virtual Account • Virtual Account Structure • Virtual Identifier • Virtual Account Structure • Create Invoice • Bulk Bill Upload

Field Name	Description
Accounting Type	Accounting type of transaction: The accounting type can be: • SDSC: Single Debit Single Credit • SDMC: Single Debit Multi Credit • MDMC: Multi Debit Multi Credit This field does not appear for **Demand Draft Payees**, **Domestic Payees**, **Internal payees**, **International Payee** and **Mixed Payees, Invoice and Virtual Account** templates.
File Type	The file type - delimited or fixed length.
Format Type	The format in which file is uploaded. The format could be .CSV, .XML, .XLS, .XLSX.
Approval Type	The approval type is at file level or record level. • File Level - The approver accepts or rejects the entire file, and all records are either processed or rejected en-masse. • Record Level - The approver could approve some records, and rejects others. Payments are processed only for approved records.
Access Type	The access type is at Private or Public. • Public- all users belonging to the party can access the identifier by default. • Private- file identifier is not accessible to every users belonging to the party. To map the required file identifier to a specific user or a set of users, refer to **"User File Identifier Mapping"** screen

10. Click **Edit** to modify the file identifier.
    OR
    Click **Back** to navigate to the previous screen.
    OR
    Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.

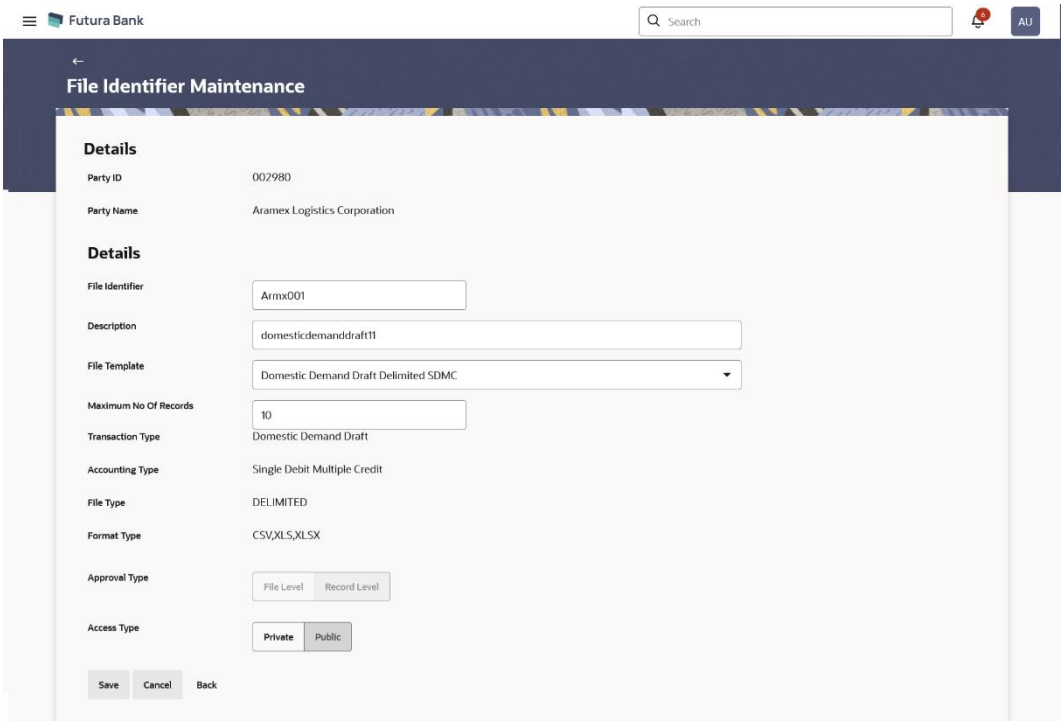
52.1.6 File Identifier Maintenance - Corporate User - Create

Using this option the administrator user can create a new file identifier.

To create a file identifier:

11. In the **Party Id** field, enter the party id of the user.
    OR
    In the **Party Name** field, enter the name of the party.
12. Click **Search**. The **File Identifier Maintenance** screen with search results appears.
    OR
    Click **Clear** to clear the search parameters.
    OR
    Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
13. Click **Create**. The **File Identifier Maintenance - Create** screen appears.

File Identifier Maintenance - Create



Field Description

Field Name	Description
Party ID	Party id for whom the file identifier is created.
Party Name	Party name corresponding to the party id.
Details	
File Identifier	Unique code or name assigned to the uploaded file.
Description	Descriptions corresponding to the file identifier.

Field Name	Description
File Template	Predefined file templates. Following file templates are available: • Domestic Funds Transfer Delimited SDSC • Domestic Funds Transfer Fixed SDSC • Domestic Funds Transfer Delimited MDMC • Domestic Funds Transfer Fixed MDMC • Domestic Funds Transfer Delimited SDMC • Domestic Funds Transfer Fixed SDMC • Domestic Funds Transfer Delimited SDSC with Account ID defined at File Identifier level • Internal and Domestic Funds Transfer Delimited SDMC • Internal and Domestic Funds Transfer Fixed SDMC • Internal Funds Transfer Delimited SDSC • Internal Funds Transfer Fixed SDSC • Internal Funds Transfer Delimited MDMC • Internal Funds Transfer Fixed MDMC • Internal Funds Transfer Delimited SDMC • Internal Funds Transfer Fixed SDMC • Internal Funds Transfer Delimited SDMC with Account ID defined at File Identifier level • Internal Funds Transfer Delimited SDSC with Account ID defined at File Identifier level • International Funds Transfer Delimited SDSC • International Funds Transfer Fixed SDSC • International Funds Transfer Delimited MDMC • International Funds Transfer Fixed MDMC • International Funds Transfer Delimited SDMC • International Funds Transfer Fixed SDMC • Demand Draft Payees • Domestic Payees • Internal payees • International Payees

Field Name	Description
	• Mixed Payees • Mixed Payments Delimited MDMC • Mixed Payments Fixed MDMC • Mixed Payments Delimited SDSC • Mixed Payments Fixed SDSC • Create Virtual Accounts • Create Virtual Accounts Structure • Create Virtual Identifier • Create Invoice • Bulk Bill Upload
Maximum No of Records	Maximum number of records permissible in the uploaded file.
Partial Processing Tolerance (%)	The partial processing tolerance for a file (in percentage terms). Suppose, the user sets this value at 60% - this implies that if 60% or more, of the records in a file clear the Validation stage, then the file can go for further processing. If less than 60% of the records in a file clear the validation stage, then the file is rejected. This field is enabled if approval is 'Record Type'.
Debit Account Number	Account number from where amount has to be debited. This field appears for templates having **AcctId defined at FI level**.

Field Name	Description
Transaction Type	Type of transaction: The Transaction type could be: • Internal Funds Transfer • Domestic Funds Transfer • International Funds Transfer • Mixed Transfer • Internal Payee • Domestic Payee • International Payee • Mixed Payee • Domestic Demand Draft Payee • International Demand Draft Payee • Virtual Account • Virtual Account Structure • Virtual Identifier • Virtual Account Structure • Create Invoice • Bulk Bill Upload
Accounting Type	Accounting type of transaction. The accounting type could be: • SDSC: Single Debit Single Credit • SDMC: Single Debit Multi Credit • MDMC: Multi Debit Multi Credit This field does not appear for **Demand Draft Payees**, **Domestic Payees**, **Internal payees**, **International Payee, Mixed Payees, Invoice and Virtual Account** templates.
File Type	The file type – delimited or fixed length.
Format Type	The format in which file is uploaded. The format could be CSV, XML, XLS, XLSX.

Field Name	Description
Approval Type	The approval type is at file level or record level. • File Level - The approver accepts or rejects the entire file, and all records are either processed or rejected en-masse. • Record Level - The approver could approve some records, and reject others. Payments are processed only for approved records. Note: Approval Type cannot be modified once it is created.
Access Type	The access type is at Private or Public. • Public- all users belonging to the party can access the identifier by default. • Private- file identifier is not accessible to every users belonging to the party. To map the required file identifier to a specific user or a set of users, refer to **"User File Identifier Mapping"** screen

14. In the **File Identifier** field, enter the code of the file to be maintained for upload.
15. In the **Description** field, enter the file description corresponding to the file code.
16. From the **File Template** list, select the file template.
    a. If you have selected a file template with **AcctId defined at FI level** from the **File Template** list, enter the Debit Account Number.
17. Select the appropriate **Approval Type**.
18. Select the appropriate **Access Type.**
19. Click **Save**.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
    OR
    Click **Back** to navigate to the previous screen.
20. The **File Identifier Maintenance - Review** screen appears. Verify the details and click **Confirm**.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
    OR
    Click **Back** to navigate to the previous screen.
21. The success message appears along with the transaction reference number and status. Click **OK** to complete the transaction and navigate back to 'Dashboard'.

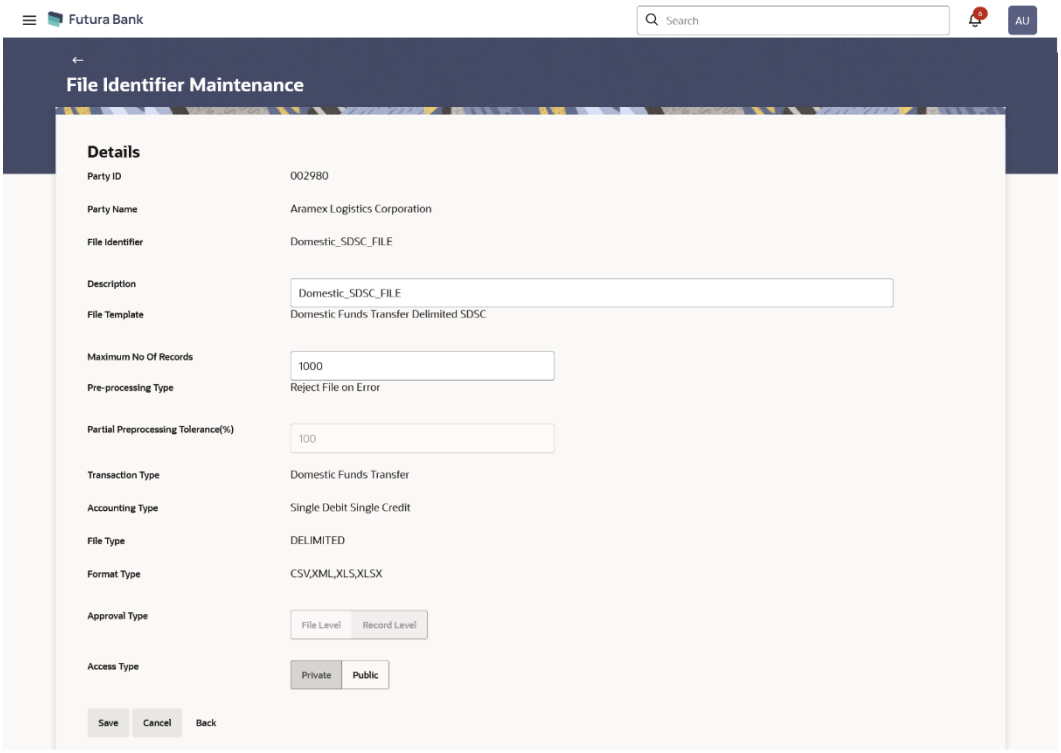
52.1.7 File Identifier Maintenance - Corporate User – Edit

Using this option the administrator can edit and update a file identifier.

To edit file identifier:

22. In the **Party Id** field, enter the party id of the user.
    OR
    In the **Party Name** field, enter the name of the party.
23. Click **Search**. The **File Identifier Maintenance** screen with search results appears.
    OR
    Click **Clear** to clear the search parameters.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
24. Click the file identifier record.
    The **File Identifier Maintenance- View** screen appears.
25. Click **Edit** to edit the file identifier mapping.
    The **File Identifier Maintenance - Edit** screen appears.

File Identifier Maintenance - Edit



26. Edit the required fields of file identifiers. E.g. Description, Maximum Number of Records, and Partial Processing Tolerance, Debit Account Number – if required.

User Interface Details

Field Name	Description
Description	Descriptions corresponding to the file upload code.
Maximum No of Records	Maximum Number of records permissible in the uploaded file.
Partial Processing Tolerance (%)	The partial processing tolerance for a file (in percentage terms) Suppose, the user sets this value at 60% - this implies that if 60% or more, of the records in a file clear the Validation stage, then the file can go for further processing. If less than 60% of the records in a file clear the validation stage, then the file is rejected.

27. Click **Save** to save the modified details.
    OR
    Click **Back** to navigate to previous screen.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
28. The **File Identifier Maintenance – Edit - Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
    OR
    Click **Back** to navigate to the previous screen.
29. The success message appears along with the transaction reference number and status. Click **OK** to complete the transaction and navigate back to 'Dashboard'.

FAQ

1. **For bank administrators which transactions have file upload support?**

   Currently the file upload feature for bank administrators is available for addition of billers only.

2. **What are the different transaction types, accounting types and file formats supported?**

   The following table details the different transaction types, accounting types and file formats supported. A file identifier with a specific template is a combination of the parameters below:

Sr. No.	Parameter	Types
1	Transaction Type	Internal funds Transfer Domestic Funds Transfer International Funds Transfer Mixed Transfer Admin Biller (available only for admin user) Payee Files (Internal / Domestic / International Or Mixed Payee Files) Virtual Account related (Accounts, Structure & Identifiers creation) Invoice Creation Bulk Bill Upload
2	Accounting Type	Single Debit, Single Credit (SDSC) Single Debit, Multi Credit (SDMC) Multi Debit, Multi Credit (MDMC)
3	Approval Type	File Level Record Level
4	Format Type	CSV, XML, XLS, XLSX

3. **Why do we have different accounting types?**

   File templates support different accounting types, and business users can use the template that best support their needs. Details with business examples below:

Sr No.	Accounting Type	Business Example	Approval Type
1	Single Debit, Single Credit (SDSC)	A corporate may want to make monthly payments to its various vendors from one central account. So though the debit account is the same across all records, the credit accounts are different and the debit accounting entry is not consolidated.	Record Type or File Type
2	Single Debit, Multi Credit (SDMC)	A corporate may want to make monthly salary payments to all its employees. A single consolidated debit entry is required to be passed, against multiple credits to different accounts.	File Type
3	Multi Debit, Multi Credit (MDMC)	This file format caters to a lot of one to one transfers between two parties for various payments. Organizations that are brokers or intermediaries in trade contracts, may find this format more suitable for their business needs.	Record Type

4. What is the business rationale of having different approval types?

A record type approval, gives more flexibility to the corporate user – in the sense, that even if some records are not validated, the file could still be processed (only those records that have passed validations) and file type approval, gives more control to the corporate user. Since all records in the file have to pass validations, before a file is processed.

5. Who can create File Identifiers for a corporate party?

Only a bank administrator or a corporate administrator with required rights can create file identifiers for a corporate party.

6. What is a 'File Upload Template'?

A template that is used to upload a file is called as file template. It distinguishes one file from another depending on:

a) Transaction type of the file

b) Format of the file to be uploaded

c) Approval type set-up for the file

d) Accounting type of a payment file

52.2 User File Identifier Mapping

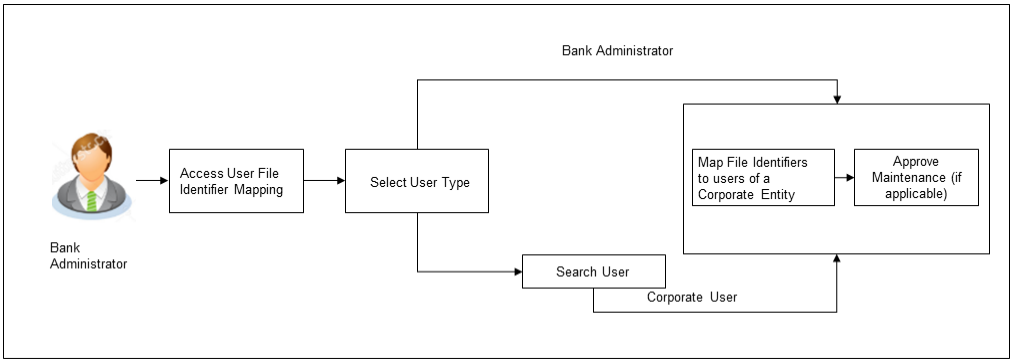
This function can be used by the administrator to map the required file identifier to a specific user or a set of users so that the user can upload and view the required file types. In case of corporate user the mapping will be done for the Party ID and for bank administrators mapping will be done for the User ID.

Prerequisites

- Transaction access is provided to Bank Administrator User Creation
- Party and Account access (for corporate file upload)
- Set up Transaction and account access (for corporate file upload)
- Set up Approval Rules (for corporate file upload)
- File Identifier Maintenance

Features Supported In Application

- Search User File Identifier Mapping
- Create User File Identifier Mapping
- Edit User File Identifier Mapping



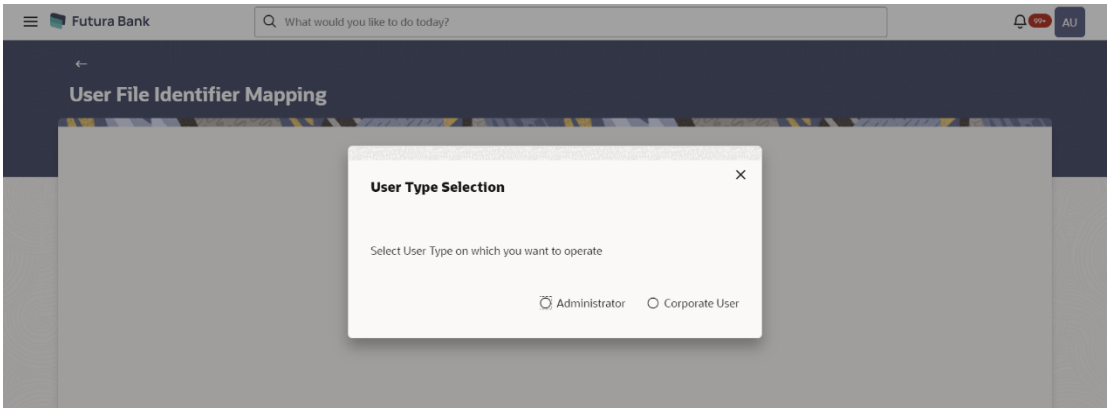
How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > File Upload > User File Identifier Mapping
OR
Bank Administrator Dashboard > Quick Links > File Upload > User File Identifier Mapping
OR
Search Bar > File Upload - User File Identifier Mapping

52.2.1 User File Identifier Mapping – User Type Selection

Bank Administrator logs into the system and navigates to the User File Identifier Mapping screen. On accessing the ‘User File Identifier Mapping’ menu, bank administrator has to select the user type.

User File Identifier Mapping – User Type Selection



1. Click **Administrator** to access file identifier for bank administrator users. The User File Identifier Mapping screen appears.
2. Click **Corporate User** to access the file identifier of corporate users. The User File Identifier Mapping screen appears.

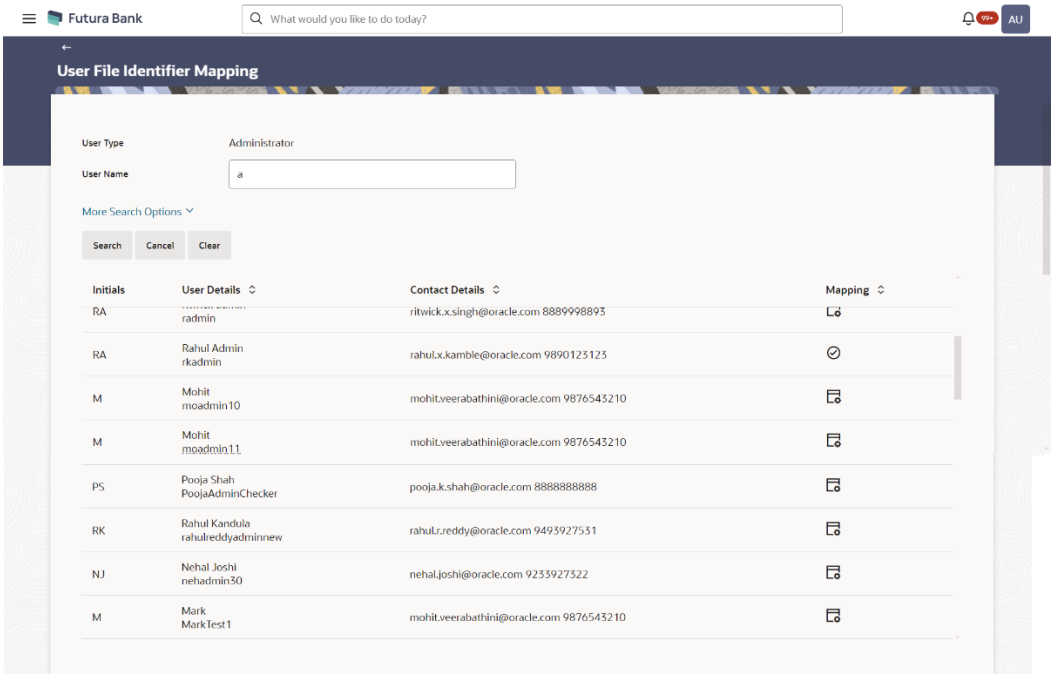
52.2.2 User File Identifier Mapping – Administrator - Search

Using this option the administrator can search and view the file identifiers mapped to the user.

To search and view the file identifiers:

1. In the **User File Identifier Mapping** screen, enter any one search criteria.
2. Click **Search**. The **User File Identifier Mapping** screen with search results appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Clear** to clear the search parameters.

User File Identifier Mapping - Search



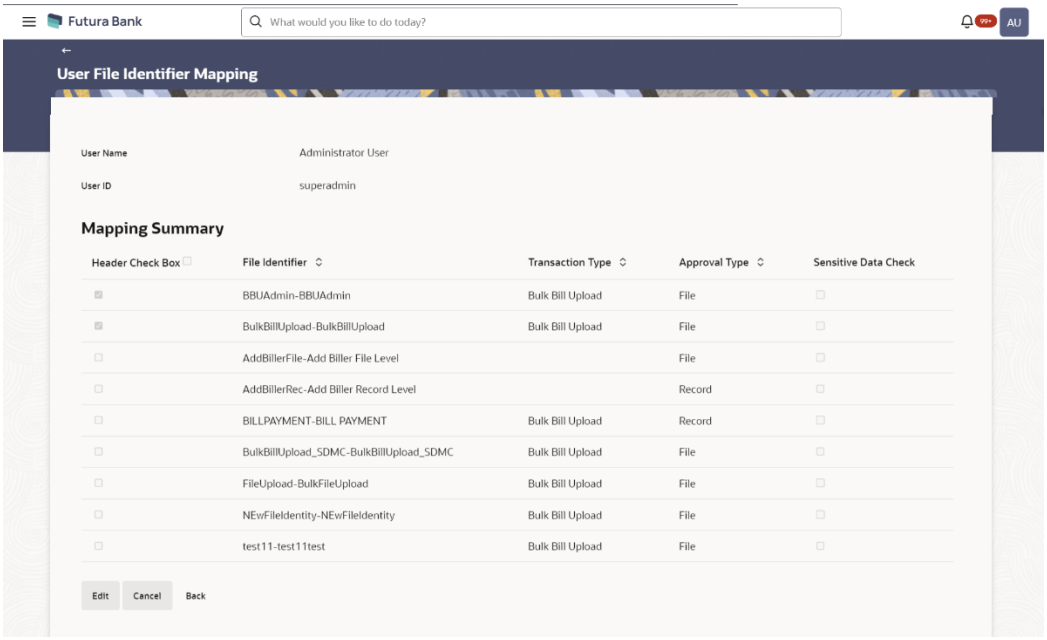
Field Description

Field Name	Description
User Type	The type of user as selected in the User File Identifier Mapping – User Type Selection screen. The options are: • Administrator • Corporate User
User Name	To search the user with the user name. Partial search is allowed.

Field Name	Description
More Search Options	
Below fields appears if you click the **More Search Options** link.	
First Name	To search based on first name or given name of the user.
Last Name	To search based on last name/ surname of the user.
Email	To search based on email id of the user.
Mobile Number	To search based on mobile number of the user.
Search Result	
Initials	The initials of the user.
User Details	The details of the user like user name or user id.
Contact Details	Email and contact number of the user.
Mapping	Displays whether the file identifier is mapped to the user. • - denotes that the file identifier is mapped to the user • - denotes that the file identifier is not mapped to the user.

3. Click against the file identifier record of which you want to view the details. The **User File Identifier Mapping - View** screen appears.

User File Identifier Mapping - View



Field Description

Field Name	Description
User Name	User name of the logged-in user.
User Id	User id of the user.
Mapping Summary	
Header Check Box	The check box to select the records for mapping.
File Identifier	Unique code assigned to the uploaded file.
Transaction Type	Type of transaction: The transaction type could be: • Admin Biller
Approval Type	The approval type is at file level or record level. • File Level - The approver accepts or rejects the entire file, and all records are either processed or rejected • Record Level - The approver could approve some records, and reject others. Payments are processed only for approved records

Field Name	Description
Sensitive Data Check	If selected, the users are barred from viewing the contents of the file.

4. Click **Edit** to modify the user file identifier mapping.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to navigate to the previous screen.

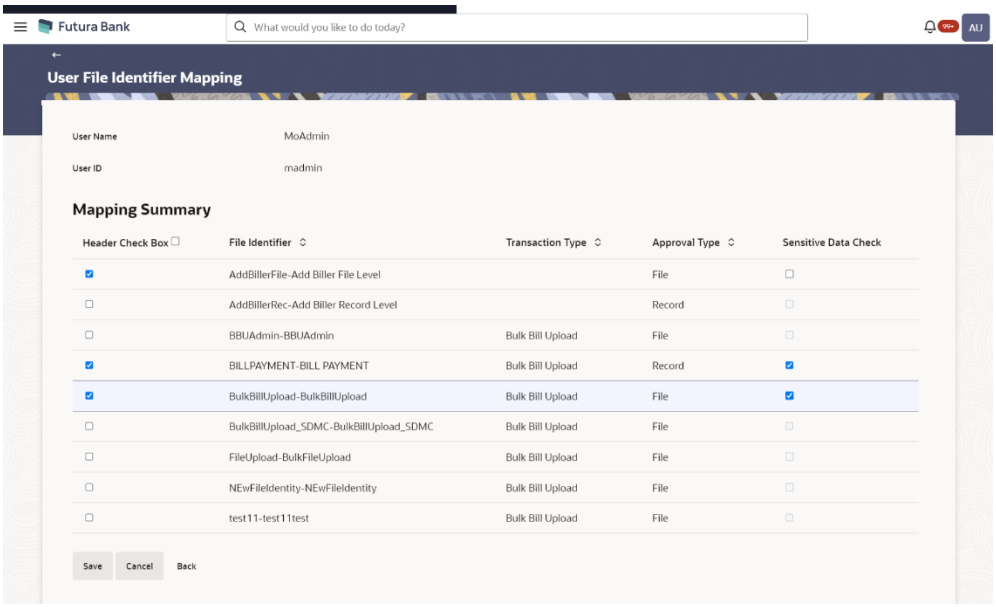
52.2.3 User File Identifier Mapping – Administrator - Create

Using this option the administrator can map the file identifiers to a user.

To map a user to a file identifier:

1. In the User File Identifier Mapping screen, enter any one search criteria.
2. Click **Search**. The **User File Identifier Mapping** screen with search results appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Clear** to clear the search parameters.
3. Click against the file identifier record, for which you want to map the user. The **User File Identifier Mapping** screen appears.

User File Identifier Mapping - Create



Field Description

Field Name	Description
User Name	User name.
User Id	User id of the user.
Mapping Summary	
Header Check Box	The check box to select the records for mapping.
File Identifier	Unique code assigned to the uploaded file.
Transaction Type	Type of transaction: The Transaction type could be: • Bulk Bill Upload
Approval Type	The approval type is at file level or record level. • File Level - The approver accepts or rejects the entire file, and all records are either processed or rejected •
Sensitive Data Check	If selected, the users are barred from viewing the contents of the file.

4. In the **Mapping Summary** section, select the file identifier which you want to map to the user.
5. Check / Uncheck the **Sensitive Data** check field, to enable / disable access to the contents of the file.
6. Click **Save**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.
7. The **User File Identifier Mapping - Review** screen appears. Verify the details and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.
8. The success message appears along with the transaction reference number and status of the transaction.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

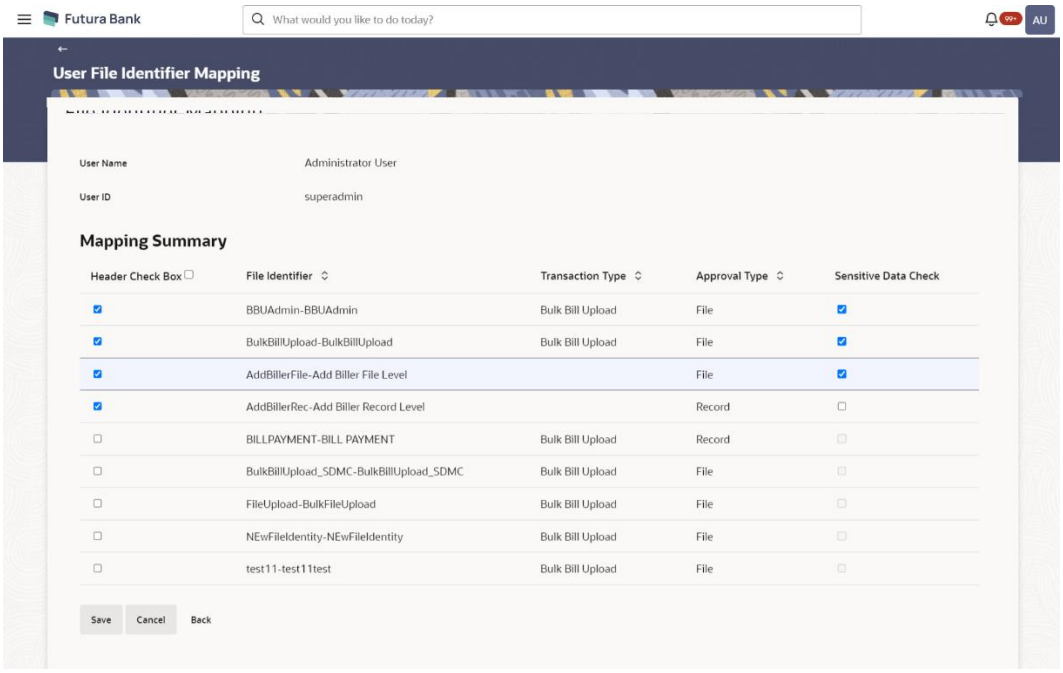
52.2.4 User File Identifier Mapping – Administrator - Edit

Using this option the administrator can edit and update mapping of a file identifier, to a user

To edit a User File Identifier Mapping:

1. In the **User Name** field, enter the username of the user.
2. Click **Search**. The **User File Identifier Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
3. Click against the file identifier record. The **User File Identifier Mapping - View** screen appears.
4. Click **Edit**. The **User File Identifier Mapping - Edit** screen appears.

User File Identifier Mapping - Edit



5. View the details of File Identifier mapping already saved. Select or de-select the File Identifier record to map / un-map a File Identifier to a user.
6. Check / Uncheck the Sensitive Data Check, to enable / disable the complete access to file content.
7. Click **Save** to save the modified details.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to navigate to previous screen.
8. The **User File Identifier Mapping - Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to navigate to previous screen.
9. The success message appears along with the transaction reference number and status of the transaction.
   Click **OK** to complete the transaction and navigate back to ‘Dashboard’.

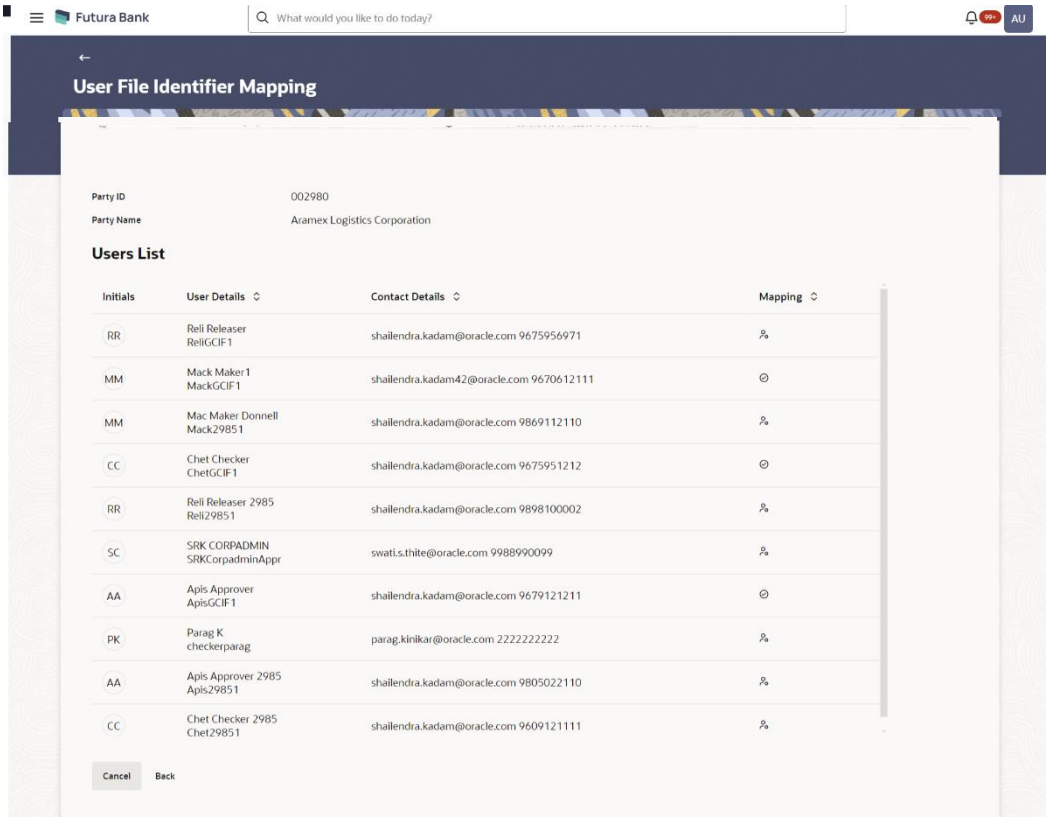
52.2.5 User File Identifier Mapping - Corporate User - Search

Using this option bank administrator can search and view the file identifiers mapped to the corporate user.

To search and view the file identifiers:

1. In the **Party Id** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the name of the party.
2. Click **Search**. The **User File Identifier Mapping** screen with search results appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Clear** to clear the search parameters.

User File Identifier Mapping - Search



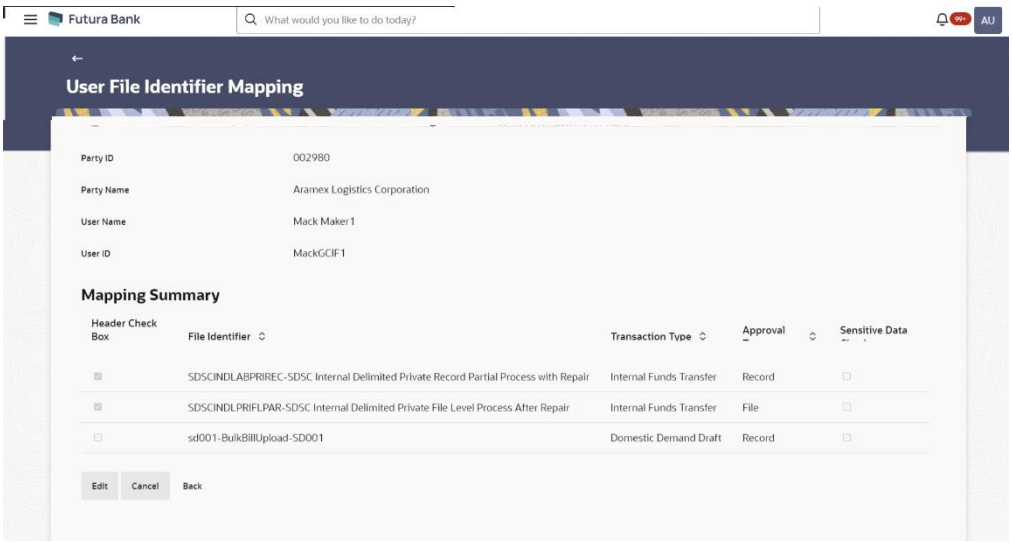
Field Description

Field Name	Description
Party ID	**Party ID of the user.**

Field Name	Description
Party Name	**Party name corresponding to the party ID.**
Users List	
Initials	The initials of the user.
User Details	The details of the user like user name or user id.
Contact Details	Email and contact number of the user.
Mapping	Displays whether the file identifier is mapped to the user. • - denotes that the file identifier is mapped to the user • - denotes that the file identifier is not mapped to the user

3. Click against the file identifier record of which you want to view the details. The **User File Identifier Mapping - View** screen appears.
   OR
   Click **Back** to go back to previous screen.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.

User File Identifier Mapping - View



Field Description

Field Name	Description
User Name	User name of the logged-in user.
User Id	User id of the user.
Mapping Summary	
File Identifier	Unique code assigned to the uploaded file.
Transaction Type	Type of transaction: The transaction type could be: • Internal Funds Transfer • Domestic Funds Transfer • International Funds Transfer • Mixed Transfer • Internal Payee • Domestic Payee • International Payee • Mixed Payee • Domestic Demand Draft Payee • International Demand Draft Payee • Create Virtual Accounts • Create Virtual Accounts Structure • Create Virtual Identifier • Create Invoice • Bulk Bill Upload
Approval Type	The approval type is at file level or record level. • File Level - The approver accepts or rejects the entire file, and all records are either processed or rejected • Record Level - The approver could approve some records, and reject others. Payments are processed only for approved records
Sensitive Data Check	If selected, the users are barred from viewing the contents of the file.

4. Click **Edit** to modify the user file identifier mapping.
   OR

Click **Back** to navigate to the previous screen.
OR
Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.

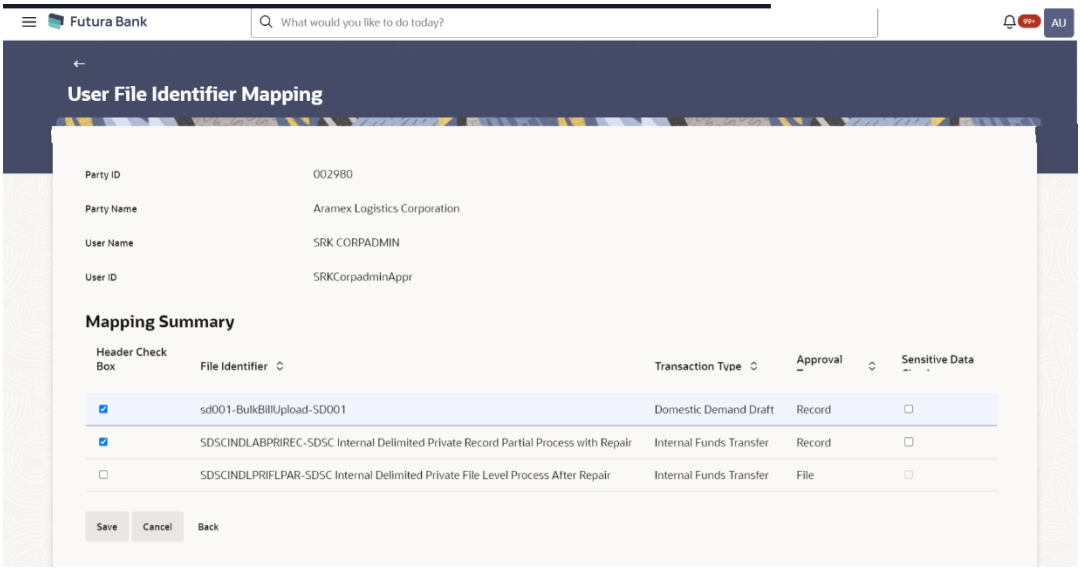
52.2.6 User File Identifier Mapping - Corporate User - Create

Using this option the administrator can map the file identifiers to a user.

To map a user to a file identifier:

1. In the **Party Id** field, enter the party id.
   OR
   In the **Party Name** field, enter the name of the party.
2. Click **Search**. The **User File Identifier Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
3. Click against the file identifier record, for which you want to map the user. The **User File Identifier Mapping** screen appears.

User File Identifier Mapping - Create



Field Description

Field Name	Description
Party ID	Party ID of the user
Party Name	Party name corresponding to the party ID.
User Name	User name.
User Id	User id of the user.
Mapping Summary	
File Identifier	Unique code assigned to the uploaded file.
Transaction Type	Type of transaction: The Transaction type could be: • Internal Funds Transfer • Domestic Funds Transfer • International Funds Transfer • Mixed Transfer • Internal Payee • Domestic Payee • International Payee • Mixed Payee • Domestic Demand Draft Payee • International Demand Draft Payee • Create Virtual Accounts • Create Virtual Accounts Structure • Create Virtual Identifier • Create Invoice • Bulk Bill Upload
Approval Type	The approval type is at file level or record level. • File Level - The approver accepts or rejects the entire file, and all records are either processed or rejected • Record Level - The approver could approve some records, and rejects others. Payments are processed only for approved records
Sensitive Data Check	If selected, the users are barred from viewing the contents of the file.

4. In the **Mapping Summary** section, select the file identifier which you want to map to the user.
5. Check / Uncheck the **Sensitive Data** check field, to enable / disable access to the contents of the file.
6. Click **Save**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.
7. The **User File Identifier Mapping - Review** screen appears. Verify the details and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.
8. The success message appears along with the transaction reference number and status of the transaction.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

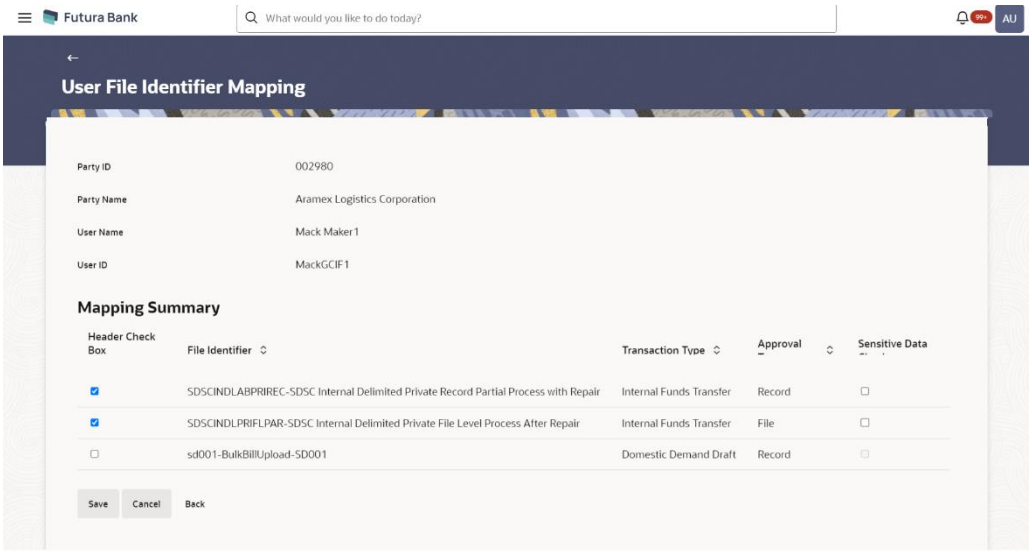
52.2.7 User File Identifier Mapping - Corporate User - Edit

Using this option the administrator can edit and update mapping of a file identifier, to a user

To edit a User File Identifier Mapping:

1. In the **Party Id** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the name of the party.
2. Click **Search**. The **User File Identifier Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
3. Click against the file identifier record. The **User File Identifier Mapping - View** screen appears.
4. Click **Edit**. The **User File Identifier Mapping - Edit** screen appears

User File Identifier Mapping - Edit



5. View the details of File Identifier mapping already saved. Select or de-select the File Identifier record to map / un-map a File Identifier to a user.
6. Check / Uncheck the **Sensitive Data Check**, to enable / disable the complete access to file content.
7. Click **Save** to save the modified details.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to navigate to previous screen.
8. The **User File Identifier Mapping - Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the operation and navigate back to ‘Dashboard’.
   OR
   Click **Back** to navigate to previous screen.
9. The success message appears along with the transaction reference number and status of the transaction.
   Click **OK** to complete the transaction and navigate back to ‘Dashboard’.

FAQ

1. **Can all users of a particular corporate access all file types, mapped to the corporate?**

   User/s have to be mapped to file identifiers to be able to access files. For example, only the user/s of Human Resource Department of a corporate may have access to upload / view and enquire status of salary files.
   Mapping File Identifier's to specific users thus enables access of certain types of file/s to certain user/s.

2. **If a user is mapped to a File Identifier and he has uploaded a file – but after this, he is no longer mapped to the File Identifier – can he view the status of the file?**

   No, the user will not be able to view the status of the file, if he is not mapped to it, at the point in time when he is checking for the status.

FAQ

1. What are some of the validations that a file goes through at various stages, in its life cycle?

The following are the validations performed on an uploaded file by OBDX and subsequently by the Host, before file is liquidated.

Sr No	Events	Applicable to	Checks
1	On File Upload	All Files	File contents should not match an already uploaded file
2	On File Upload	All Files	File should not exceed the Maximum Size limit
3	On File Upload	All Files	The File Extension type should be the ones permitted
4	On File Upload	All Files	The file should not be Malicious
5	At Pre-Processing	All Files	The format for all fields, should be as templated viz., Date, Currency in accordance with ISO standards, Party - numeric, account number-alphanumeric etc.
6	At Pre-Processing	All Files	The Party should be valid, should exist
7	File At Pre-Processing	All Files	Party and Debit account should belong to each other
8	At Pre-Processing	All Files	User should have access to Debit Account (If applicable for the type of file selected)
9	At Pre-Processing	All Files	Debit account should not be in closed status (If applicable for the type of file selected)
10	At Pre-Processing	All Files	Transaction Limits are not violated at user level (If applicable for the type of file selected)
11	At Pre-Processing	All Files	Payment date should not be in the past (If applicable for the type of file selected)
12	At Pre-Processing	All Files	Payment date should not be a holiday as per the host calendar maintenance (If applicable for the type of file selected)

Sr No	Events	Applicable to	Checks
13	At Pre-Processing	All Files	Debit account should be a CASA account, not loan or TD (If applicable for the type of file selected)
14	At Pre-Processing	All Files	Debit currency in the file, should match the currency of the CASA account (If applicable for the type of file selected)
15	At Pre-Processing	Internal Files	Transaction currency should match either the debit or credit CASA (If applicable for the type of file selected)
16	At Pre-Processing	Internal Files	The Credit Account should be a CASA account, not loan or TD (If applicable for the type of file selected)
17	At Pre-Processing	All SDSC and SDMC files	A file with multiple records, should have the same debit account (If applicable for the type of file selected)
18	At Pre-Processing	Internal Ad hoc	The Purpose of remittance should be valid (If applicable for the type of file selected)
19	At Pre-Processing	Domestic Files	The NEFT / RTGS code should be valid (If applicable for the type of file selected)
20	At Approval	All Files	Cumulative limits should not be violated either for the Approver and the Party (If applicable for the type of file selected)
21	Validations in Core	All Files	The Debit account should have sufficient balance (If applicable for the type of file selected)
22	Validations in Core	All Files	Debit account should not be in dormant status (If applicable for the type of file selected)
23	Validations in Core	All Files	Debit account should not be in debit block status (If applicable for the type of file selected)
24	Validations in Core	Internal Files	The Credit CASA account should not be closed (If applicable for the type of file selected)

Sr No	Events	Applicable to	Checks
25	Validations in Core	Internal Files	There should not be a Credit Block on the CASA account (If applicable for the type of file selected)
26	Validations in Core	International Files	The BIC / SWIFT code should be valid, as per the BIC / Clearing directory as maintained in the host system (If applicable for the type of file selected)

2. If some records in a file are liquidated, others are deleted, what will the status of the file be?

The following table shows the file status which is followed to depict various status of the file upload. So if all the records of file are liquidated then the file status is processed, and if any of the records in the file is liquidated while all the other are rejected the file status will be processed, and if any of the records is liquidated and rest all have an error the file status will be processed with exception.

Verified	Approved	Processing in Progress	Liquidated	Rejected	Deleted	Error	File Status
All							Verified
	All						Approved
		All					Processing in Progress
			All				Processed
				All			Rejected
					All		Deleted
						All	Error
			1	1			Processed
			1		1		Processed
			1			1	Processed with exception
			1	1	1		Processed

Verified	Approved	Processing in Progress	Liquidated	Rejected	Deleted	Error	File Status
			1	1	1	1	Processed with exception
				1	1		Deleted
				1		1	Processed with exception
					1	1	Processed with exception

3. **If a payment file is in the approved status, does it mean that all the records are successfully liquidated?**

   No, the file still has to successfully pass validations in the host system, before records are processed.

4. **Can a user delete the entire file or deletion of only individual records within a file is allowed?**

   Whether only records can be deleted, or the entire file will be deleted depends on the accounting type of the file, and the approval type (Record Level or File level)

   The table below throws light on the combinations allowed

Sr No	Accounting Type	Authorization Type	File / Record Deletion allowed?
1	SDMC	File Level	Not allowed
2	SDSC	File Level	Not allowed
3	SDSC	Record Level	Only records can be deleted, and not the entire file
4	MDMC	Record Level	Only records can be deleted, and not the entire file

5. **If a working window is set for the File Upload transaction – how will processing be impacted outside of the working window?**

   Outside of the transaction working window set for file uploads, processing will depend on whether the file has a Record Level approval or a File Type approval.

Files with a File Type approval – will be rejected, outside of the transaction working window
Files with Record Type approval – if some records are processed within the working window, will be completed – if processing of some records, falls outside of the working window – these will be rejected.

6. What is the impact of limits on processing of File Upload transactions?

File uploads transaction will utilize limits depending on if the transfer is an internal, domestic, or international funds transfer.
Further, for domestic funds transfer – limits are defined for each network – NEFT, RTGS and IMPS. Limits will be checked at the pre-processing's stage for file uploads.

7. After a file is successfully uploaded, is the user provided notifications on its status?

Yes, Users mapped to the FI – initiators and approvers of the file, are provided with alerts / notification, as file progresses from the Uploaded stage to Approved to Processing in Progress to the Processed stage. Alternately, users can log in to view the status of the file.

10.

53. User Group Management

User group is a set of x users with similar interests and goals.

Using User Group Management option Bank administrator can maintain the user groups of Bank administrator and of corporate users of same party ID. User groups maintained by administrators for Bank administrator users and corporate users are used while creating approval workflows and approval rules.

Also the user groups created for Bank administrator type of user are used for mapping secured mail subjects. Each subject category can be linked to a group of Bank Administrator users. So that administrators will receive the mails only of the subjects mapped to the users.

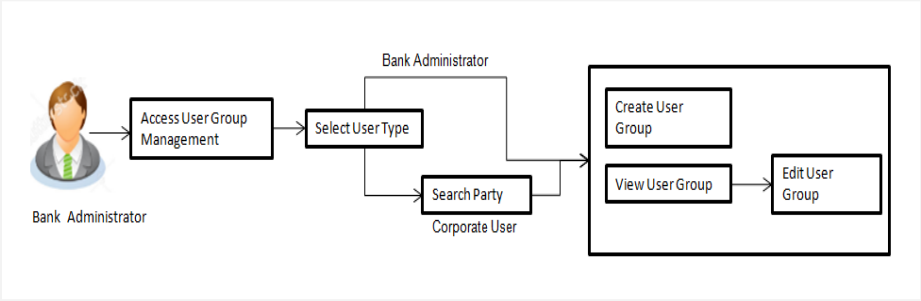
Note :

- If Group corporate Flag is set as “ON” in system rules, then the corporate users group creation will not be allowed using this menu option. The Corporate Users Group can be setup using Group Corporate onboarding only,
- If Group corporate Flag is set as “OFF” in system rules, then the corporate user group must be setup using below mentioned steps.

Prerequisites:

- Transaction access is provided to Bank Administrator.
- Multiple corporate and administrator users are maintained.
- Approval rule set up for Bank administrator to perform the actions.
- Party preference for which the groups are to be created is maintained and is active.

Workflow



Features Supported In Application

User Group Management allows Bank Administrator to:

- Create User Groups
- View User Groups

- Modify User Groups

How to reach here:

System/ Bank Administrator Dashboard > Toggle menu > Menu > Others > User Group Management

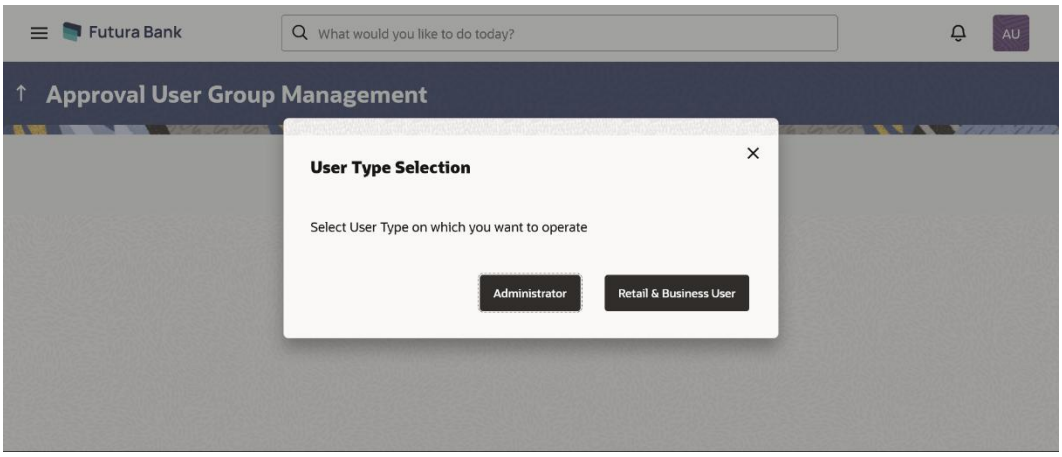
Note: User Groups can also be maintained for Non Customer Corporates (for which the party id is not maintained in UBS or in Core banking system). For such cases i.e. non customer corporate (counterparties on boarded by Corporates) the system will look for the party ID in OBSCF/OBCMS.

53.1 User Groups – Select User Type

Bank Administrator logs into the system and navigates to the User Group screen. On accessing the 'User Group Management' menu, Bank Administrator has to select the user type for whom the user groups are to be maintained.

1. The **User Type Selection** screen appears. Select the appropriate option.
   Click **Admin User** to access the user group management of Bank Administrator users.
   Click **Retail & Business User** to access the user group management of **Retail & Business** users.

User Type Selection



User Group- Admin User:

Bank Administrator user can search the user groups maintained for administrator users.

2. Click **Search** to search the matching records.
   OR
   Click **Cancel** to abort the user group maintenance process.
   OR

Click **Clear** to reset the entered details.

53.2 User Groups – Admin User

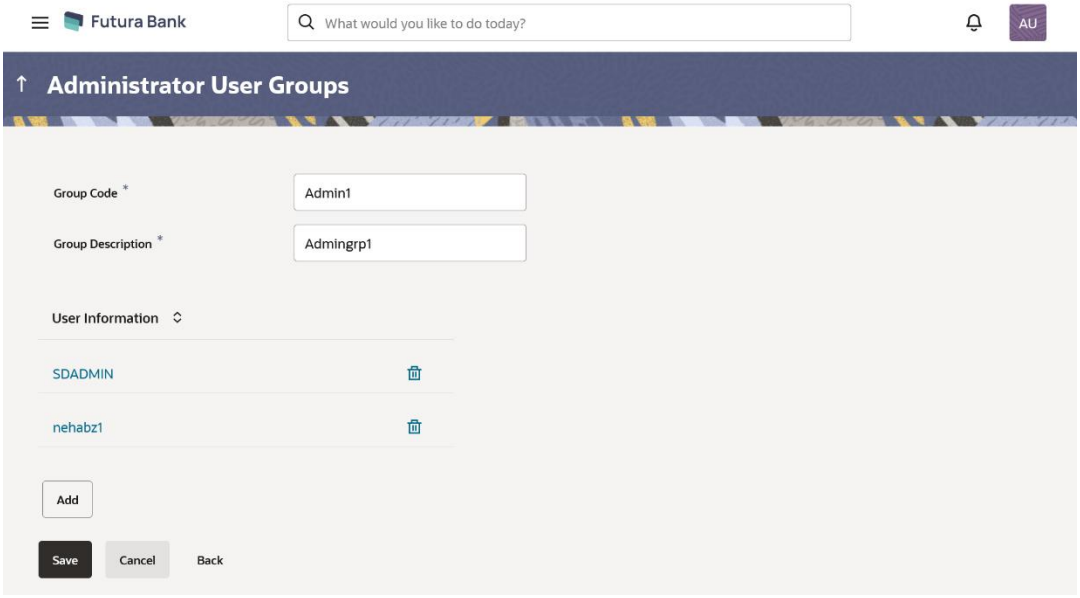
53.2.1 User Groups - Admin User – Create

Bank Administrator can create user groups for the Administrator users. Administrator can create multiple user groups and one user can be part of multiple user groups, whereas creating a user group without any user is not allowed.

To create a user group:

1. The **User selection** screen appears. Select the appropriate option.

Admin User Group -Create



Field Description

Field Name	Description
Create	
Group Code	User group code.
Group Description	Description provided to the user group.
Search Results - User Group	

Field Name	Description
User Name	User name list to select and add a user to the user group. All the administrator users will be listed down
User ID	User IDs of each user selected from user list are displayed.

2. Click **Create**.
3. In the **Group Code** field, enter the group code.
4. In the **Group Description** field, enter the group name.
5. In the **User Group** section, click **Add** to add the selected user in the User Group. Once added, the user name will be removed from the user drop-down to avoid duplication of users.
6. Click **Save** to create the user groups.
   OR
   Click **Cancel** to close the maintenance creation process.
   OR
   Click **Back** to navigate to the previous screen.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
8. The success message of user group creation appears along with the transaction reference number.
   Click **OK** to complete the transaction.

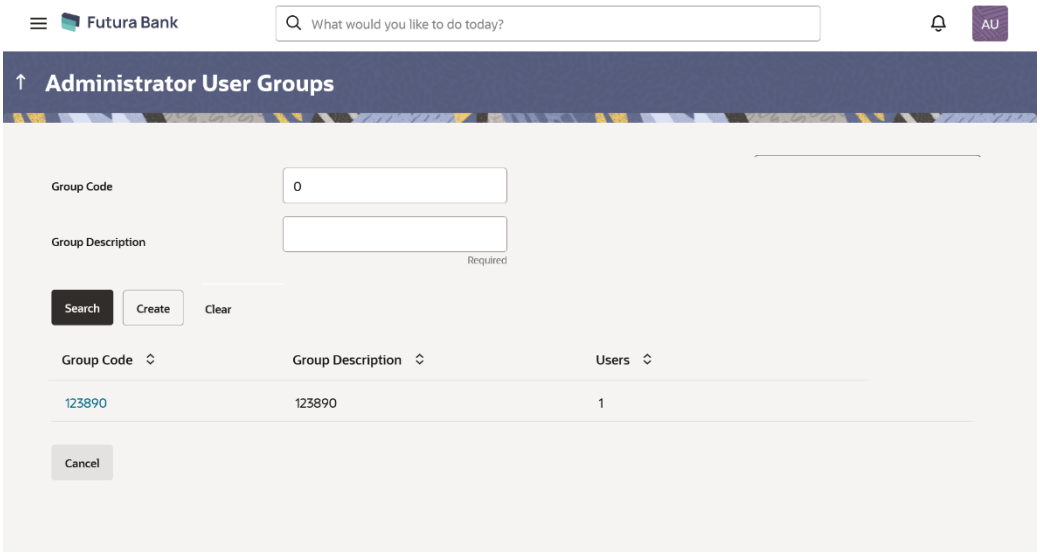
Note: You can click to delete a record.

53.2.2 User Groups - Admin User – Search Summary

User Groups maintained (if any) for administrator users are displayed on the screen after searching with valid input. User can opt to view the details of existing user groups or can create new user group using this screen.

1. In **Administrator User Group** screen, in the **Group Code** field, enter the group code.
   OR
   In the **Group Description** field, enter the group name.
2. Click **Search**. The search summary appears.

Admin User – Search Summary

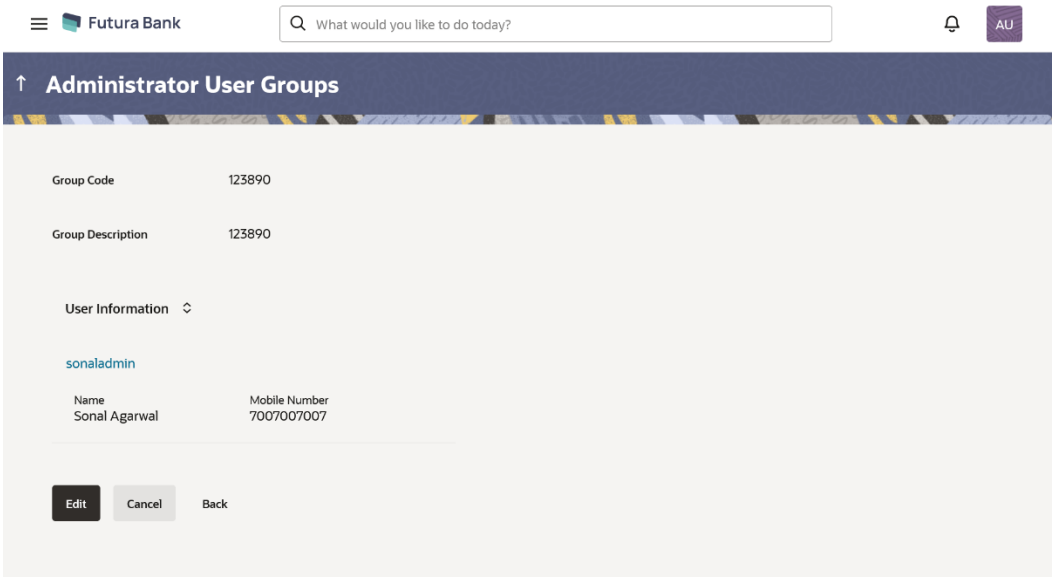


Field Description

Field Name	Description
Summary	
Group Code	Code of the already maintained user group.
Group Description	Description of the already maintained User group.
Users	Number of users associated with each user group.

3. Click **Create** to create new user group.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click on **Group Code Hyperlink** to view details of the selected User Group.
   Further drill down is given on the each user group to view the details of the users mapped to each group.

Admin User – View Group Details



Field Description

Field Name	Description
View	
Group Code	User Group code is displayed.
Group Description	User Group code description is displayed.
User Name	User name of the user who is part of the selected user group is displayed.
User ID	User ID of the user who is part of the user group is displayed.

4. Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Edit** to edit the user group. User is directed to the **User Group-Edit** screen with values in editable form.

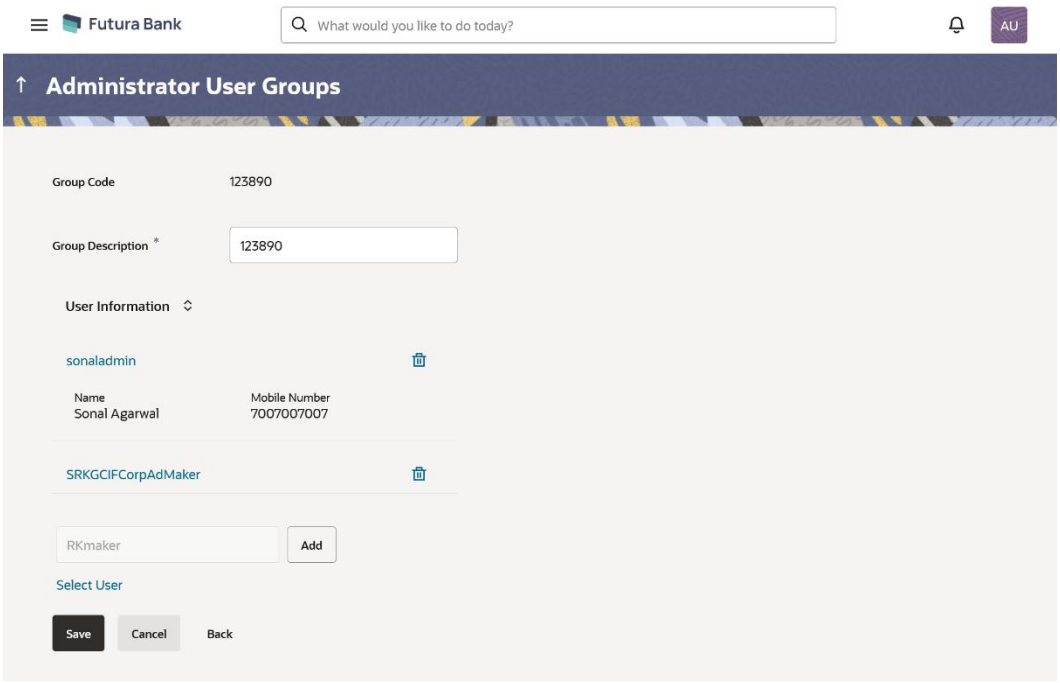
53.2.3 User Groups - Admin User – Edit Group

This function enables the Bank Administrator to edit the description of existing user groups. Bank Administrator can also add new users and remove existing users of the user group as part of this function. A check is performed on minimum and maximum number of users allowed as a part of user group while adding or removing the users from the user group.

To edit or update a user group:

1. In **Admin User Group** screen, in the **Group Code** field, enter the group code.
   OR
   In the **Group Description** field, enter the group name.
2. Click **Search**. The search summary appears.
3. Click the **Group Code** link of the record whose details you want to view.
   The **User Groups - View** screen appears.
4. Click **Edit** to edit the user group.
   The **User Groups - Edit** screen displays the mapping of the user group.

Admin User – Edit Group



Field Description

Field Name	Description
Summary	
Group Code	User Group description is displayed in editable form.
Group Description	User name of the user who is part of the user group. User name list to select and add a new user to the user group.
Users	Number of users available in each user group. (This field will be displayed only if there are existing user groups available under a party).

5. Click **Add** to add the selected user in the User Group. Once added, the user name will be removed from the user drop-down to avoid duplication of users.
   Click to remove a user from the User Group.
6. Click **Save** to save the User Group .The **User Group-Create - Review** screen post necessary validations appear.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'
   OR
   Click **Back** to cancel the operation to navigate to previous screen.
7. Verify the details, and click **Confirm**. The **User Group-Edit – Confirmation** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to cancel the operation to navigate to previous screen.
8. The success message of user group creation appears along with the transaction reference number.
   Click **OK** to complete the transaction and navigate back to 'User Groups' screen.

53.3 User Groups - Retail & Business User

53.3.1 User Groups - Retail & Business User – Search Party

Bank Administrator logs into the system and navigates to the User Group Management screen.

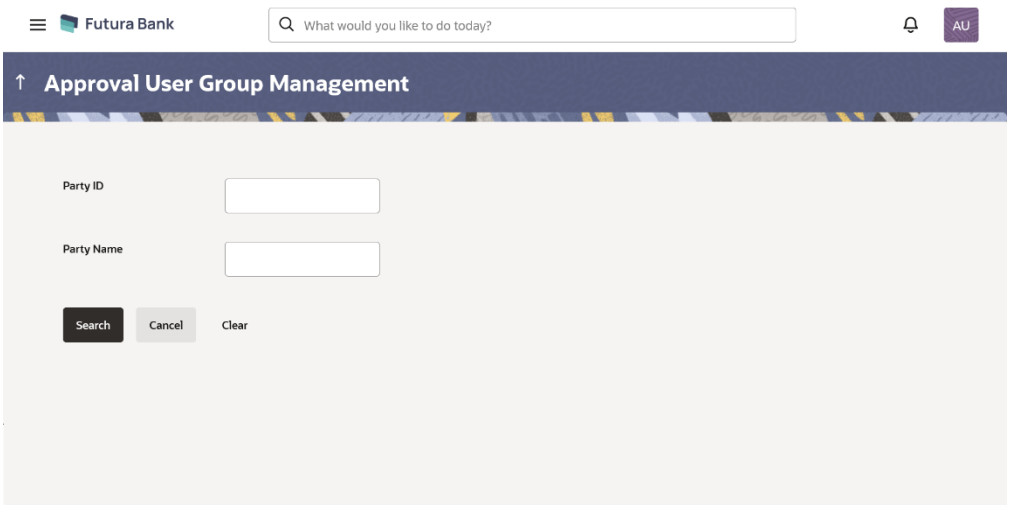
1. The **User Type Selection** screen appears. Select the appropriate option.
   Click **Retail & Business User** to access user group management of Retail & Business users.

   System displays a screen to enter the party information (party ID or party name) and search party for which the user groups are to be maintained/ viewed.

User can enter the party ID (if known) or the party name with a minimum of 5 characters. System matches the input provided by the user with the party name records and displays the matching party records.

In case of a party search by party ID, it is an exact match and system displays the user groups maintained if any.

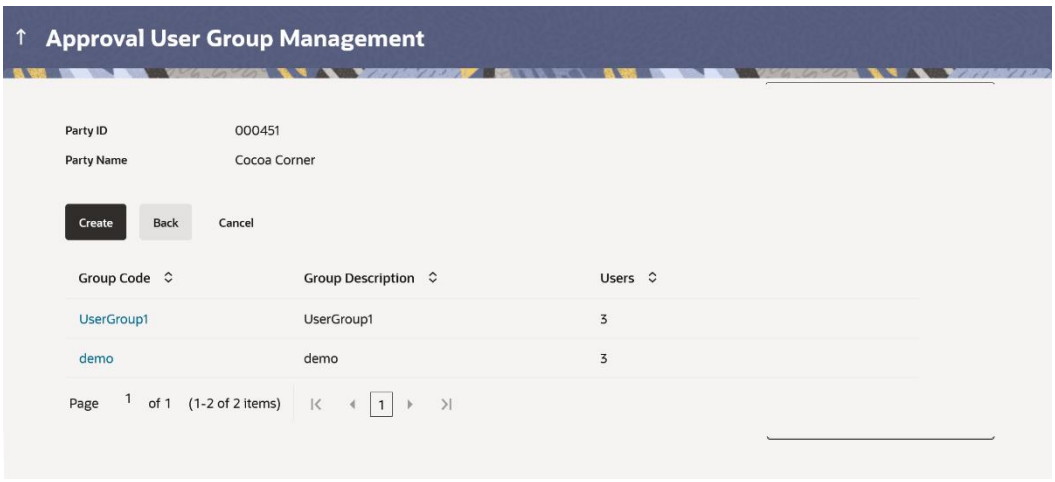
Retail & Business User – Search Party



System displays a screen to enter the party information (party ID or party name) and search party for which the user groups are to be maintained/ viewed.

In case of a party search by name, system displays the matching party records. The records have parties listed with both Party ID and Party Name information. User can select the record by clicking on the Party ID from the list.

Retail & Business User – Search by Party name



Field Description

Field Name	Description
Search	
Party ID	List of the Party IDs as per search input.
Party Name	List of the Party names of the party IDs as per search input.

2. After providing party ID or name of party, click **Search.**
   Click on **Party ID** hyperlink to view details of the selected user group.
   OR
   Click **Clear** to clear the input search parameters.
   OR
   Click **Cancel** to cancel the transaction.

53.3.2 User Groups - Retail & Business User – Create

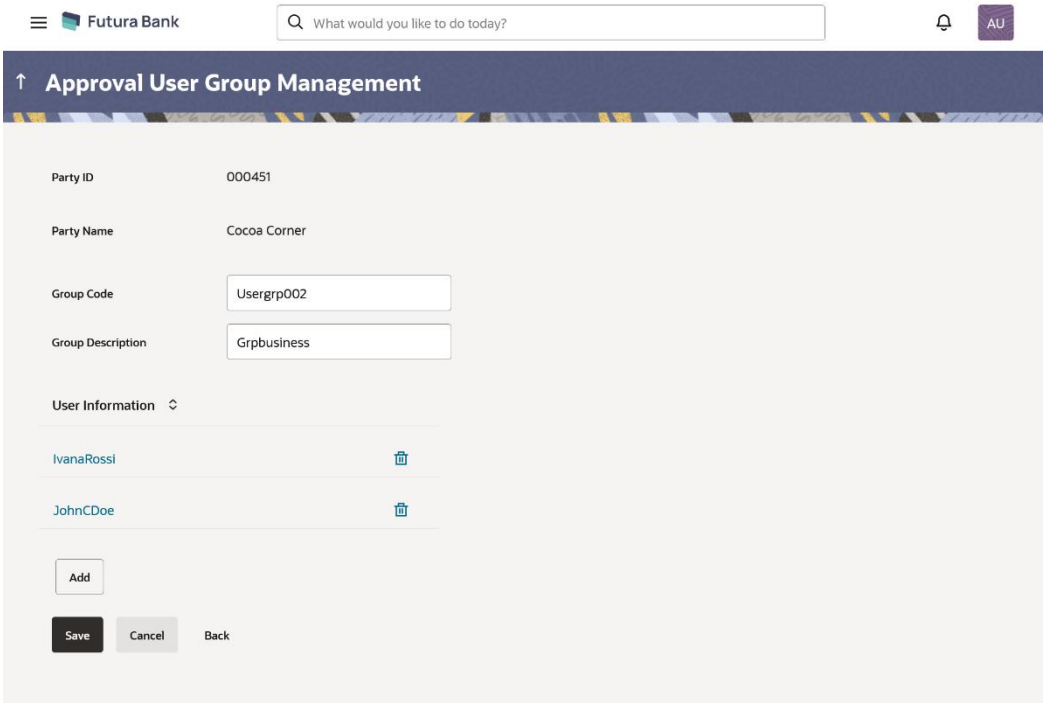
Bank Administrator can create a new User Group for a specific Party ID by using this option. Only the users of party ID can be clubbed together in a User Group.

Administrator can create multiple user groups and one user can be part of multiple user groups, whereas creating a user group without any user is not allowed.

To create a user group:

1. The **User selection** screen appears. Select the appropriate option.

Retail & Business User Group -Create



Field Description

Field Name	Description
Party ID	Party ID mapped for which user group to be created is displayed.
Party Name	Party name of Party ID for which user group to be created is displayed.
Group Code	To specify User Group code.
Group Description	To specify User Group description.

Field Name	Description
User Name	User name list to select and add a user to the user group. Users belonging to the same Party are listed.
User ID	User IDs of each user selected from user list are displayed.

2. Click **Create**.
3. In the **Group Code** field, enter the group code.
4. In the **Group Description** field, enter the group name.
5. In the **User Group** section, click **Add** to add the selected user in the User Group. Once added, the user name will be removed from the user drop-down to avoid duplication of users.
6. Click **Save** to create the user groups.
   OR
   Click **Cancel** to close the maintenance creation process.
   OR
   Click **Back** to navigate to the previous screen.
7. The **Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
8. The success message of user group creation appears along with the transaction reference number.
   Click **OK** to complete the transaction.

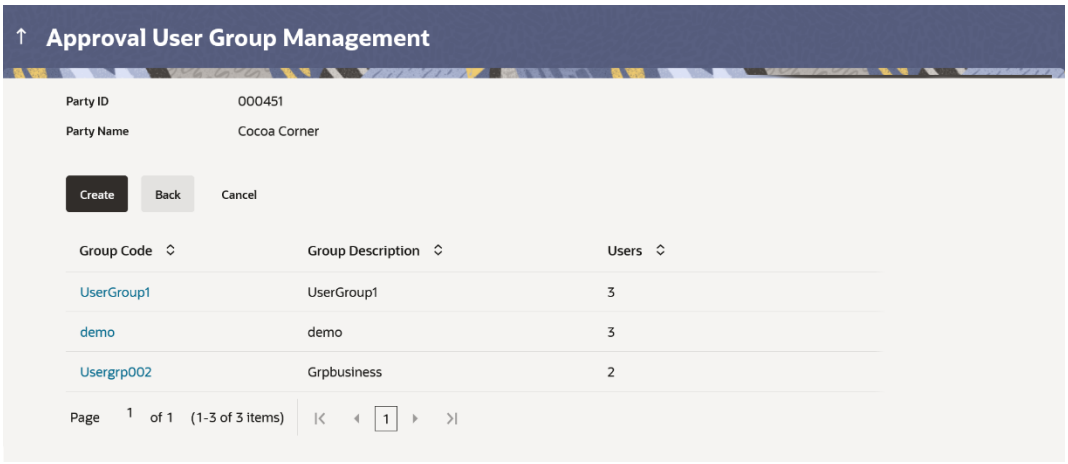
Note: You can click to delete a record.

User Groups - Retail & Business User – Group Summary

Once the logged in Bank Administrator navigates to User Group Management screen, and searches the party ID. User groups maintained if any under the party are displayed on the screen. User can opt to view the details of existing user groups or can create new user group using this screen.

1. In **User Group Management** screen, in the **Party ID** field, enter the Party ID.
2. Click **Search**. User groups maintained if any under the party are displayed on the screen.
3. Click on **Party ID** hyperlink to view details of the selected Approval Workflow.

Retail & Business User – Group Summary



Field Description

Field Name	Description
Summary	
Party ID	Party ID of which user groups are to be viewed/ edited.
Party Name	Party name of Party ID of which user groups are to be viewed/ edited.
Search Result	
Group Code	User group code. (This field will be displayed only if there are existing user groups available under a party).
Group Description	Description provided to the user group. (This field will be displayed only if there are existing user groups available under a party).
Users	Number of users available in each user group. (This field will be displayed only if there are existing user groups available under a party).

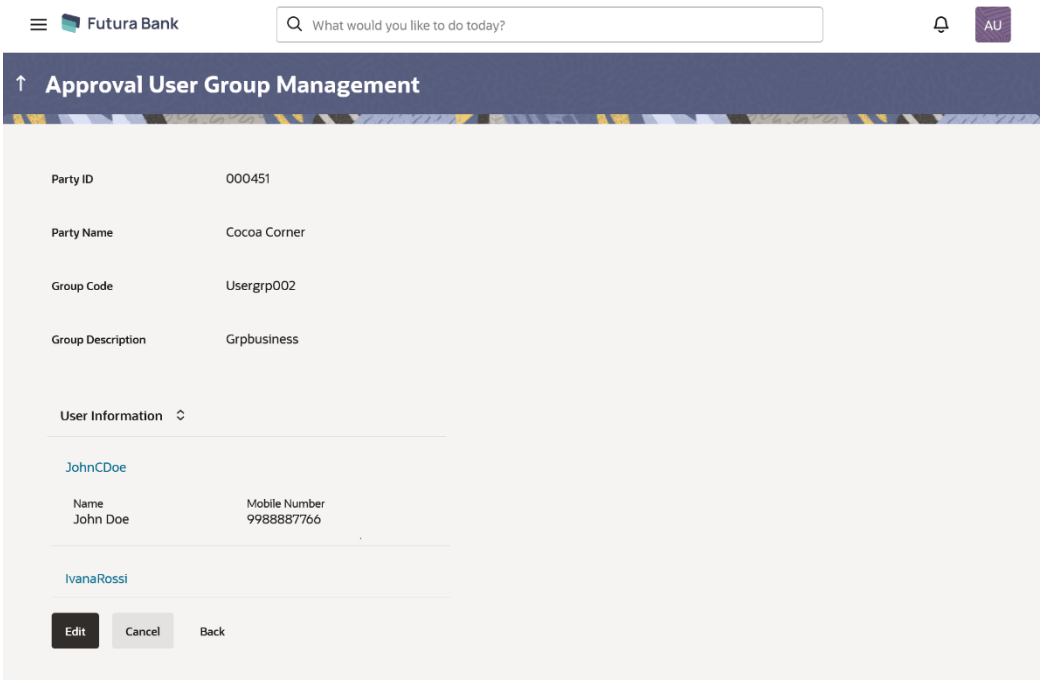
4. Click **Create** to create new user group.
   OR
   Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to abort the user group maintenance process.
   OR
   Click on **Group Code** hyperlink to view details of the selected User Group.

Further drill down is given on the each user group to view the details of the users mapped to each group.

Retail & Business User- View Group Details

On accessing ‘User Group Management’ menu option and searching the user groups of specific party, summarized view of all the user groups created (if any) for the Party is displayed on the screen. Further drill down is given on the each user group to view the details of the users who are the part of user group.

Retail & Business User – View Group Details



Field Description

Field Name	Description
View	
Party ID	Party ID of which user groups are to be viewed/ edited.
Party Name	Party name of Party ID of which user groups are to be viewed/ edited.
Group Code	User Group code is displayed.

Field Name	Description
Group Description	User Group description is displayed.
User Name	User name of the user who is part of the selected user group is displayed.
User ID	User ID of the user who is part of the user group is displayed.

5. Click **Back** to navigate to previous screen.
   OR
   Click **Cancel** to abort the user group maintenance process.
   OR
   Click **Edit** to edit the user group. User is directed to the **User Group-Edit** screen with values in editable form.

53.3.3 User Groups - Retail & Business User – Edit Group

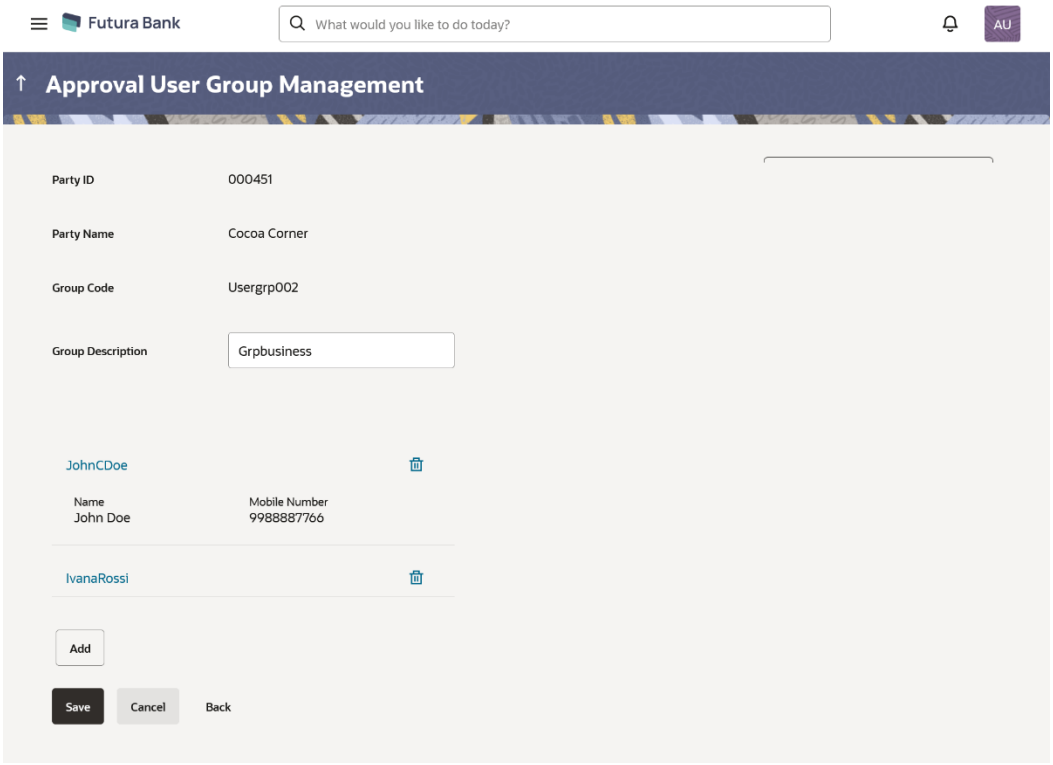
This function enables the Bank Administrator to edit the description of existing user groups. Bank Administrator can also add new users and remove existing users of the user group as part of this function.

A check is performed on minimum and maximum number of users allowed as a part of user group while adding or removing the users from the user group.

To edit or update a user group:

1. In **User Group Management** screen, in the **Party ID** field, enter the Party ID.
2. Click **Search**. User groups maintained if any under the party are displayed on the screen.
3. Click on **Party ID** hyperlink to view details of the selected Approval Workflow.
4. Click **Edit** to edit the user group.
   The **User Groups - Edit** screen displays the mapping of the user group.

Retail & Business User – Edit Group



Field Description

Field Name	Description
Edit	
Party ID	Party ID of which user groups are to be viewed/ edited.
Party Name	Party name of Party ID of which user groups are to be viewed/ edited.
Group Code	User Group code is displayed.
Group Description	User Group description is displayed in editable form.
User Name	User name of the user who is part of the user group. User name list to select and add a new user to the user group.
User ID	User ID of the user who is a part of the user group is displayed.

5. Click **Add** to add the selected user in the User Group. Once added, the user name will be removed from the user drop-down to avoid duplication of users.

   Click to remove a user from the User Group.

6. Click **Save** to save the User Group .The **User Group-Edit- Review** screen post necessary validations appear.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to cancel the operation to navigate to previous screen.
7. Verify the details, and click **Confirm**. The **User Group-Edit – Confirmation** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to cancel the operation to navigate to previous screen.
8. The success message of user group creation appears along with the transaction reference number.
   Click **OK** to complete the transaction and navigate back to 'User Groups' screen.

FAQ

1. Can a user be the part of multiple user groups created under a party?

Yes, same user can be part of multiple user groups. Whereas creating a user group without any user is not allowed.

2. Where can these Administrator User Groups be used?

User groups created for Administrator users are used for approval and for User Group – mail subject mapping.

Approval - User groups maintained by administrators are used while creating approval workflows and approval rules.

Secured Mailbox - Each subject category is linked to a group of Bank Administrator users. Depending upon the mail-subject mapping to each Bank Administrator user, administrators will receive the mails only of the subjects mapped to the users and initiated by bank's customers.

3. Can I delete an existing user group?

No, user groups cannot be deleted but can be edited. Administrator can add new users and remove existing users of the user group.

4. Can I add users of linked party ID while creating a user group for primary party?

No, only users of primary party can be the part of user group.

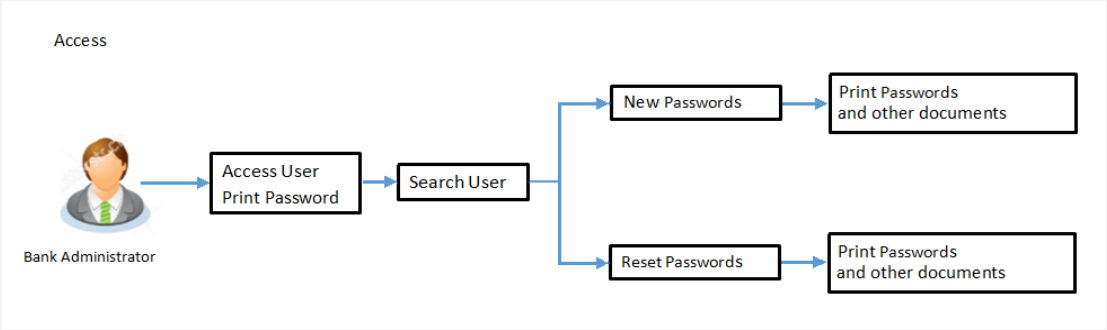
54. Print Password

When a new user opens an account in the bank and registers for channel banking, the bank sends the printed password along with some other documents like Welcome letter, Terms & Conditions document and applicable promotional offers to the registered user via courier or post. This screen allows the Bank Administrator to print the password along with these documents for new users as well as for existing users who have requested for reset password.

Pre-Requisites

- Application roles and child roles are maintained
- Transaction access is provided to Bank Administrator.

Workflow



Features Supported In Application

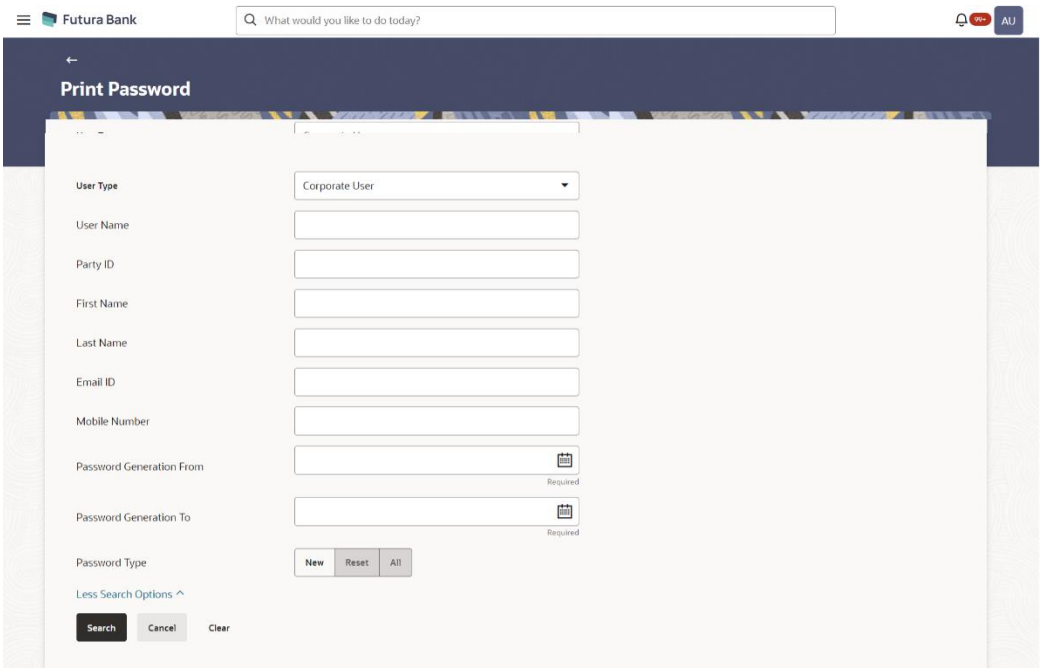
The Print Password allows the Bank Administrator to

- Print Password and other welcome documents for new and existing users

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Others > Print Password

Print Password



54.1 Print Password - Search

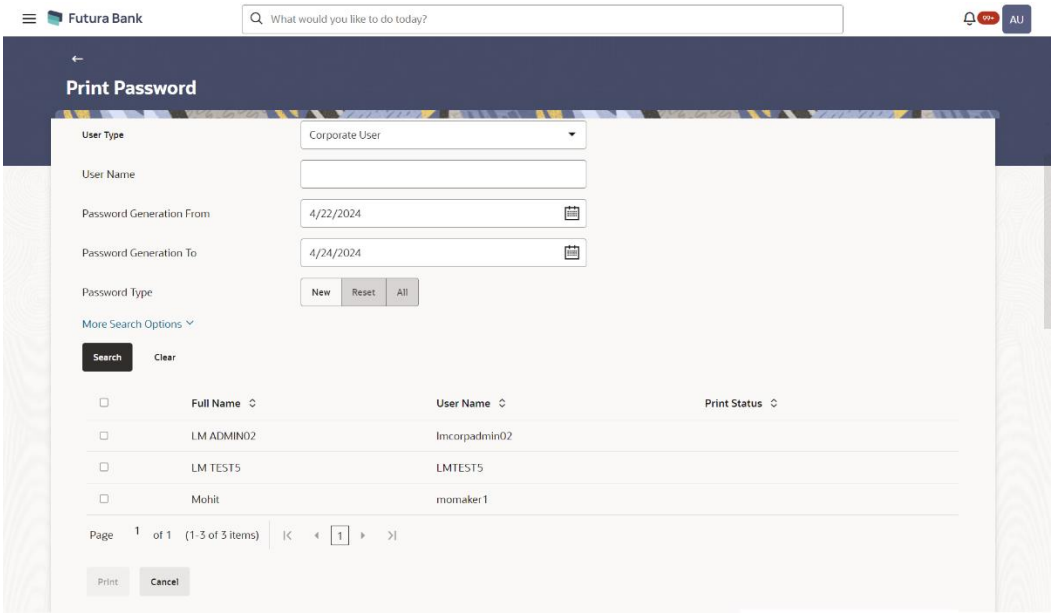
Using this option, Bank Administrators can search the users to send the printed password.

All the users (new & existing) for which the password has been generated for first time or got reset will be available on this screen. Once the password gets successfully printed for a user, that record will get removed from the list.

To search user:

1. From the **User Type** list, select the appropriate type of user.
   OR
   Click **Cancel** to cancel the transaction.
2. In the **Party ID** field, enter the party id of the user.
3. From the **Password Type** list, select the appropriate option.
4. Enter the other search criteria if required.

Print Password - Search



Field Description

Field Name	Description
User Type	Type of user, which is to be searched. The user types are: • Corporate • Retail • Administrator
User Name	To search the user with the user name. Partial search is allowed.
Party ID	Allows to search based on Party id.
First Name	Allows to search based on first name or given name of the user.
Last Name	Allows to search based on last name/ surname of the user.
Email ID	Allows to search based on email id of the user.
Mobile Number	Allows to search based on mobile number of the user.

Field Name	Description
Password Generation From	Allows to search based on password generation date.
Password Generation To	Allows to search based on password generation date.
Password Type	Allows to search based on password type. The options are: • New- Password created for new users of the bank. • Reset- Password created for the existing users of the bank who are requested for the password reset. • All- Password created for new users as well as existing users of the bank.
Search Results	
Full Name	First name and last name of the user.
User Name	User Name of the user.
Print Status	Print status of the password. If the password printing gets failed due to some reason for a user, system will show the status as 'error in printing' for that record. If the record gets successfully printed that record will get removed from the list. For the records which are not printed yet, this status remains blank.

5. Click **Search**.
   The search results appear on the **Print Password** screen based on the search parameters.
   OR
   Click **Clear** if you want to reset the search parameters.
   OR
   Click **Print** if you want to print the password letter, welcome letter, terms and conditions documents.
   OR
   Click **Cancel** if you want to cancel the transaction.

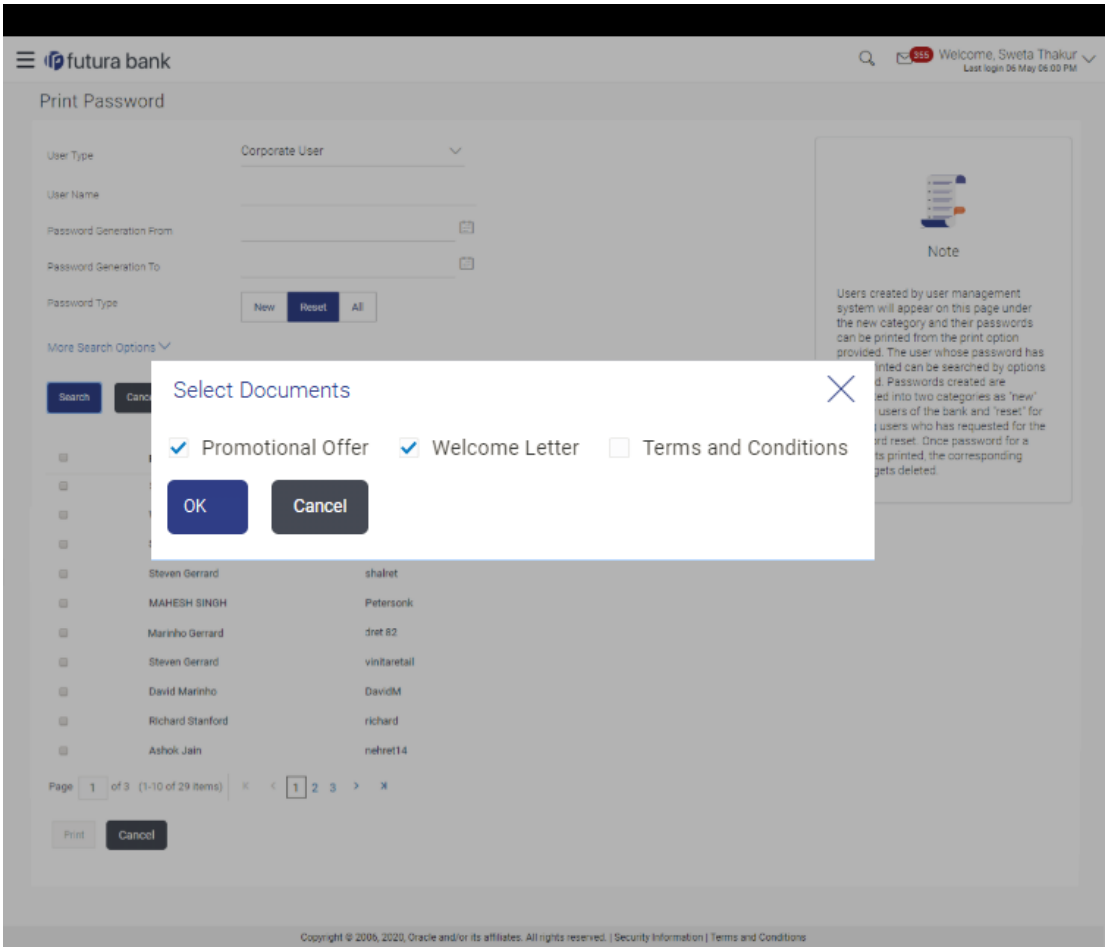
54.2 Print Password - Print

This feature allows the Bank Administrator to print the password letter, welcome letter, terms and conditions document etc.

To print the password letter for the user:

1. In the **Print Password - Search Results** section, select the user record for which you want to print the password letter.
2. Click **Print**. The 'Select Documents' pop up window appears.

Print Password



Field Description

Field Name	Description
Select Documents	
Terms & Conditions	Document containing terms and conditions of the bank.
Welcome Letter	Welcome letter for the user for opening the account.
Promotional Offer	Promotional offers of the bank.

3. Select the documents, which you desire to print.
4. Click **Print** to print the documents.
   OR
   Click **Cancel** to cancel the printing.

Note: For printing the password, the implementation team will need to write a utility. For more information on implementation of 'Print Password', refer **Oracle Banking Digital Experience Security Guide**.

FAQ

1. **Can the password be only printed by the same Administrator user who has created the user/reset the password or it can be done by any other Administrator user as well?**

   All the reset/new passwords can be printed by all the admin users who have access to Print Password Screen.

2. **Can the Bank maintain separate documents for each type of user role?**

   No, documents cannot be maintained as per the user role. Same documents will be available for all type of users (Retail/Corporate/Administrator).

55. User Alerts Subscription

Using this option System/Bank Administrator can subscribe alerts for a user for selected events. Retail and Corporate users of the bank, can contact the bank to subscribe to alerts. The Bank Administrator subscribes users to alerts, delivered through Email, SMS, through push notification or in their on-screen mailbox.

Note: This functionality is for non-mandatory alerts.

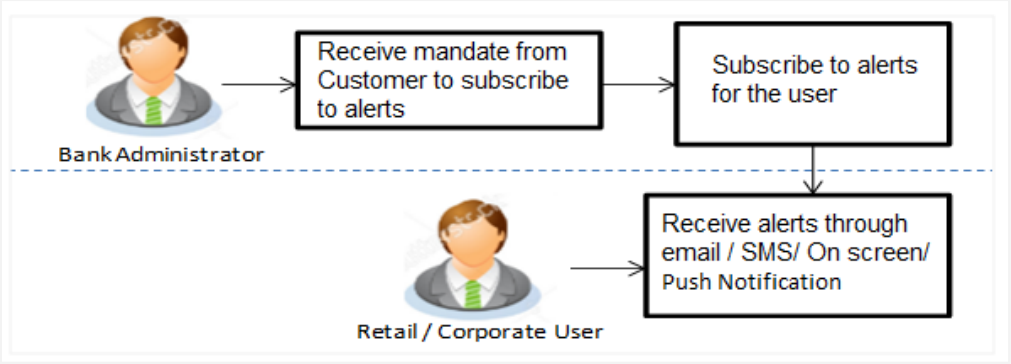
The subscribed alert types are:

- User Level Alerts
- Customer Level Alerts
- Account Level Alerts

Pre-Requisites

- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.
- Maintain Alerts, so that these are available for subscription
- Customers (retail and corporate users) are maintained

Workflow



Features Supported In Application

- Search alerts subscribed
- Subscribe / unsubscribe to alerts

How to reach here:

System/ Bank Administrator Dashboard > Toggle menu > Menu > Others > User Alerts Subscription

55.1 User Alerts Subscription - Search

Using this option, the Bank Administrator can search and view the details of alerts subscribed for the Retail or Corporate users of a Party. Here, bank admin is required to search user to whom alert maintenance is to be set up by entering party id of retail/ corporate user .

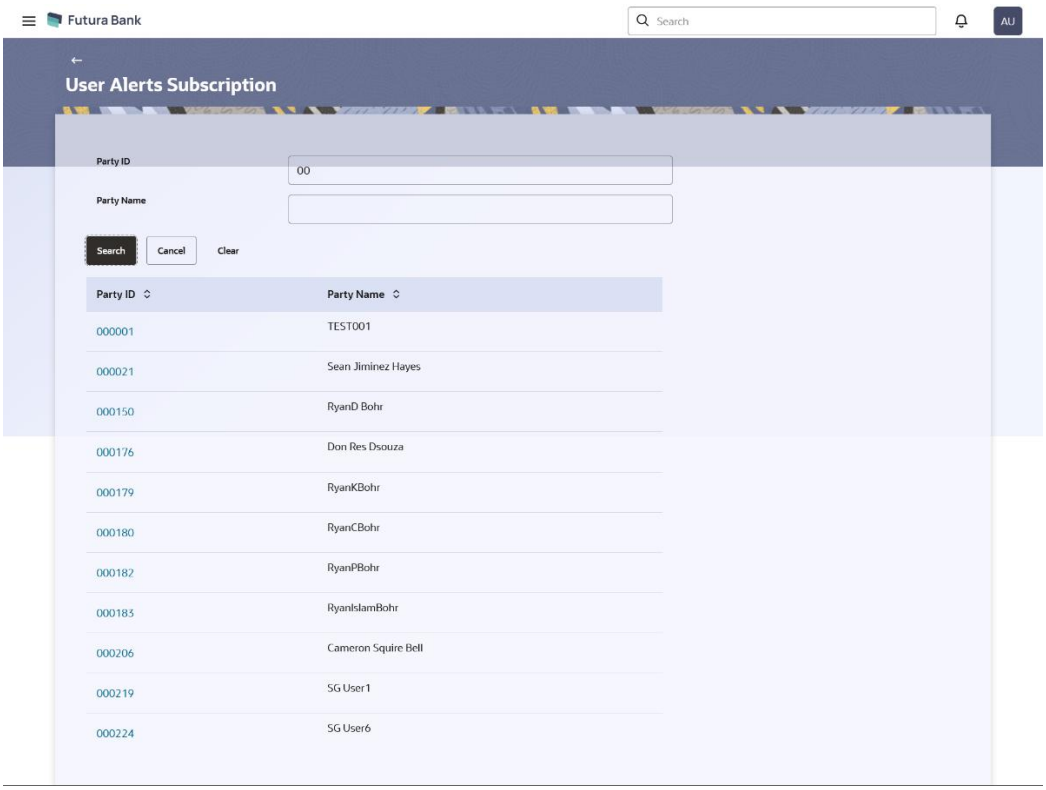
Once party id is identified application will display all the user records on boarded for selected Party Id with their Alerts Subscription Status. For the users whose alerts subscription is completed will be displayed with an indicator as alert subscription is done. Once, Admin selects the user, he will be navigated to User alert subscription detailed page.

All the alerts subscribed for a party will be displayed in the respective categories viz. Current and Savings, Term Deposits, Loans etc. in a table.

To view subscribed alerts for a Party:

1. In the **Party Id** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the name of the party.
2. Click **Search**. The party id will be displayed based on the search criteria.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.

User Alerts Subscription – Party Search



Field Description

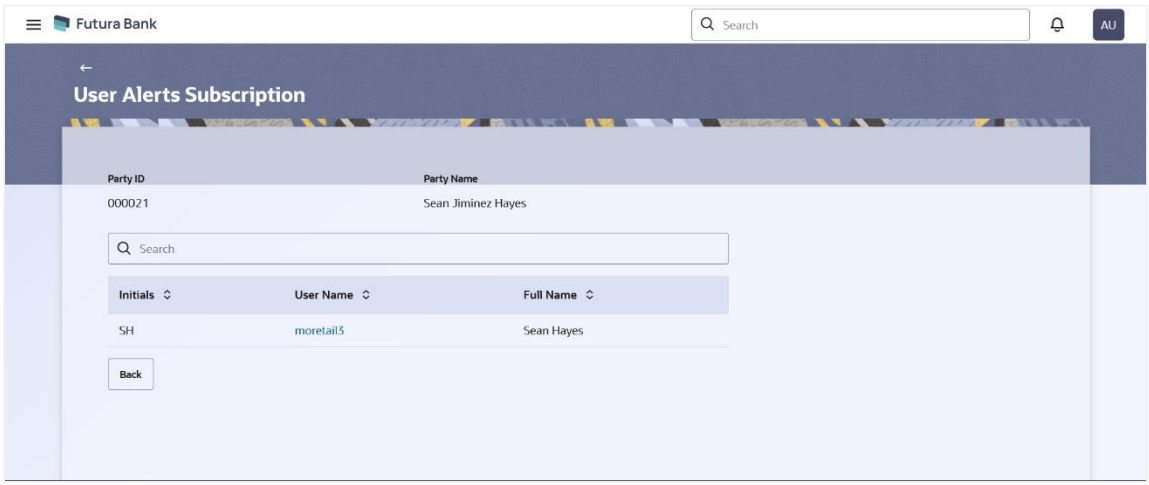
Field Name	Description
Party ID	Party Id of the user.
Search Party Name	Enter Party Id, and click to search the party name of the user.
Search Result	
Party Id	Display Party ID
Party Name	Display Party name

To view subscribed alerts for a User:

1. Click on the **Party ID** link whose alerts you wish to view. The system displays the users whose alerts subscription is completed.

Note: In the search field, enter the user name to search the specific user. The search result appears based on the search criteria.

User Alerts Subscription – User Search



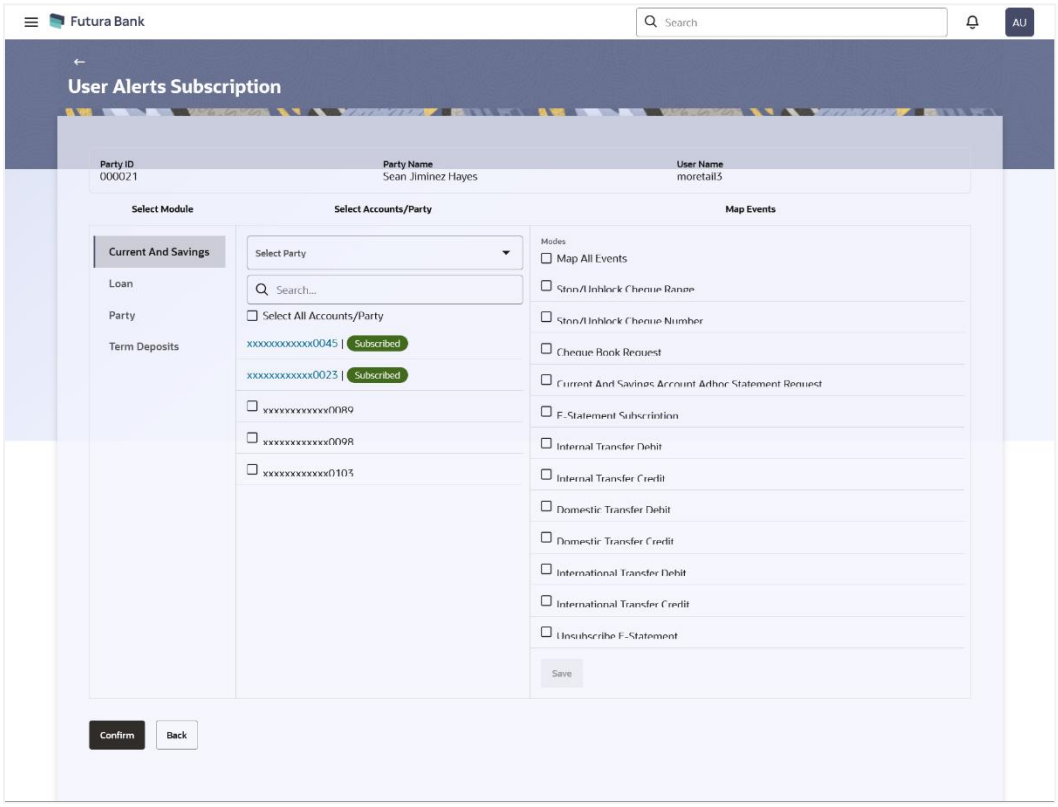
Field Description

Field Name	Description
Party ID	Display Party ID.
Party Name	Display Party name.

Field Name	Description
Search User	Enter user name maintained in the core banking application for retail users and maintained for users.
Search Result	
Initials	Display Initials of the User.
User Name	Display User Name.
Full Name	Display Corporate / Retail users Full name. **Note**: For the users whose alerts subscription is completed will be displayed with an indicator as alert subscription is done.

2. For the detailed view, click on **User Name** field. The tabs for all modules CASA/ Term Deposit/ Loans / Profile that the user has access to with the respective account numbers appears.
3. Select the particular account number to view alert type and delivery mode, for each CASA (Current and Savings Accounts) / TD (Term Deposits) / Loans account.

User Alerts Subscription - Detailed View



4. Select the checkbox against the alerts to subscribe/ unsubscribe the alerts.
5. Click **Save** to save the changes.
6. Click **Confirm** to subscribe/ unsubscribe alerts. The system displays the success message of alerts subscribed.
   OR
   Click **Back** to navigate to back to the previous screen.

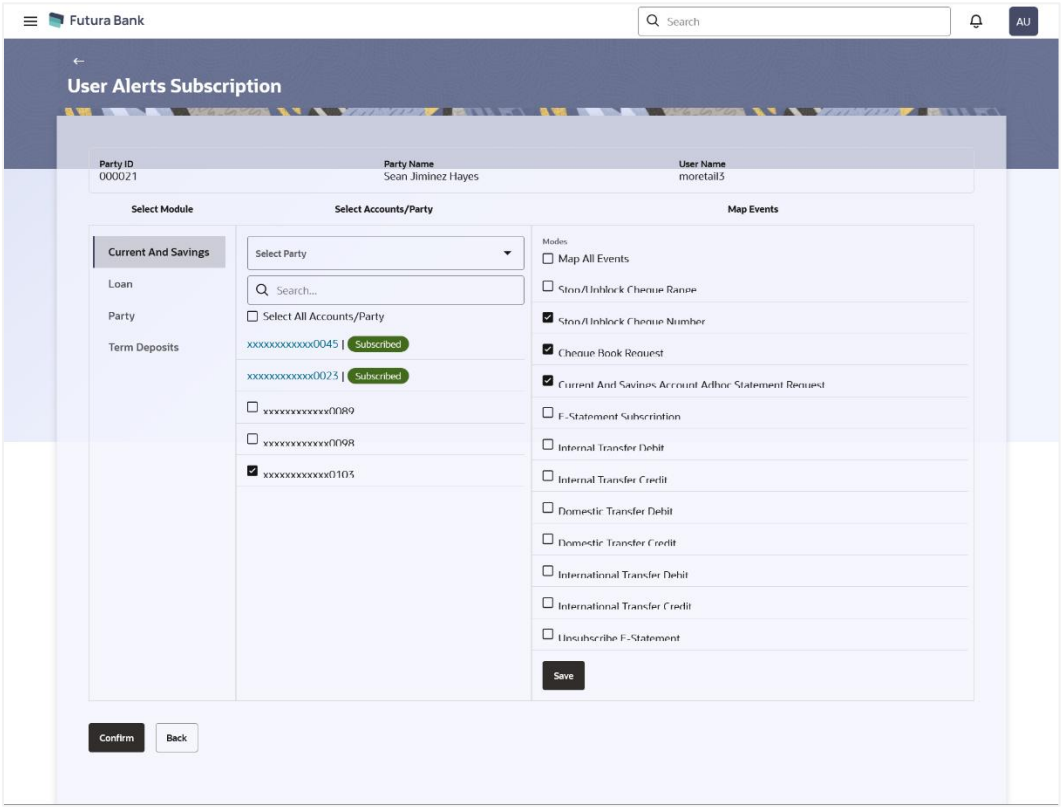
55.2 Subscribe/ Unsubscribe Alerts

Using this option, Bank Administrator can modify the alerts subscribed for the user.

To subscribe / unsubscribe alerts:

1. Repeat steps 1 to 5 of **Alerts Subscription- Search** section.
   The categories viz details of an alert subscribed appears.
2. Select the particular account number to view the alerts subscribed.

User Alerts Subscription - Subscribe / Unsubscribe



Field Description

Field Name	Description
Party ID	Party Id of the user for whom alerts to be subscribed.
Party Name	Party Name of The user.
User Name	User name maintained in the core banking application for retail users and maintained for corporate users.
Select Module	Name of the module to which alerts is maintained. The options can be: • CASA • Loan • TD • Profile • Payments

Field Name	Description
Select Accounts/Party	The Account number for which the user is viewing/ updating the alert subscription. Note: • Bank Admin will be allowed to select and setup alert subscription for multiple or all accounts in single maintenance. • Once the subscription is done for an account that account will be shown with a 'Subscribed' tag. • Bank admin will be able to quick search account number from search panel for the alert subscription OR The party under for which the user is viewing/ updating the alert subscription.
Select All Accounts /Party	The option to select all accounts/party at once.

CASA /TD/ Loans/ Payments

Subscribed alerts displayed in tabs for all modules that the user has access to with the respective account numbers.

3. Select the checkbox against the alerts to subscribe/ unsubscribe the alerts.
4. Click **Save** to save the changes.
5. Click **Confirm** to subscribe/ unsubscribe alerts. The system displays the success message of alerts subscribed.
   OR
   Click **Back** to navigate to back to the previous screen.

To view the list of events for Alert, click here.

FAQ

1. **Which alerts can the Bank Administrator subscribe or unsubscribe, for the retail or corporate user?**

   The alerts which are not mandatory can be subscribed or unsubscribed, by the Bank Administrator for the retail/corporate user.

2. **What if a Retail or Corporate customer wants to opt-out of alerts?**

   The Bank Administrator can unsubscribe the alerts for a Retail or Corporate customer. Please note that the customer will continue to receive the mandatory alerts irrespective of his choice on the subscribed alerts.

56. Group Corporate Alerts Subscription

Using this option System/Bank Administrator can subscribe alerts at the Group Corporate level for selected events. The Bank Administrator subscribes the Corporate Party associated with Group Corporate to alerts, delivered through Email, SMS, through push notification or in their on-screen mailbox.

If Group Corporate Alerts Subscription has been maintained for particular corporate Party, then the same will be inherited to the users of that corporate party and will be available at User Alert subscription for any modification.

Incase User Alert Subscription is not maintained for a user and Group Corporate Alerts subscription is maintained then system will read whatever is maintained at the corporate Party level.

If both Party and User level subscription is not maintained, no alerts will be sent to the user.

Note that this functionality is for non-mandatory alerts.

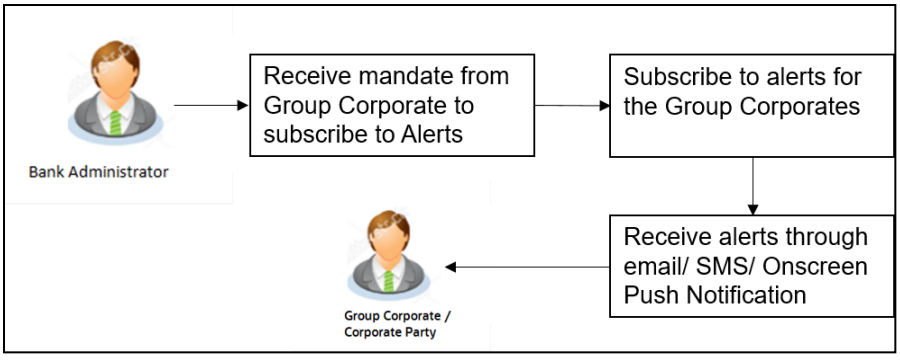
The subscribed alert types are:

- Group Corporate Level Alerts
- Party Level Alerts
- Account Level Alerts

Pre-Requisites

- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.
- Maintain Alerts, so that these are available for subscription
- Party Preferences is maintained

Workflow



Features Supported In Application

- Search alerts subscribed
- Subscribe / unsubscribe to alerts

How to reach here:

System/ Bank Administrator Dashboard > Toggle menu > Menu > Others > Group Corporate Alerts Subscription

56.1 Group Corporate Alerts Subscription - Search

Using this option, the Bank Administrator can search and view the details of alerts subscribed for the Corporate Party associated with Group Corporate. Here, bank admin is required to search Group corporate for whom the alert maintenance is to be set up by entering Group Corporate ID or Group Corporate Name.

Once the Group Corporate is identified, application will navigate the user to Alerts Subscription detailed page. Here user can select the corporate party associated with Group Corporate from the available list and Application will display their current Alerts Subscription Status.

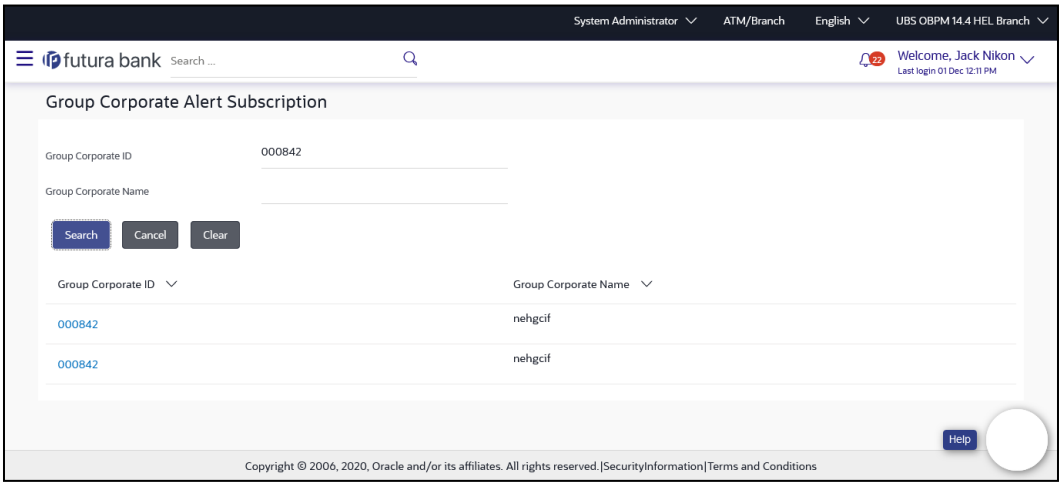
For the Corporate Parties whose alerts subscription is completed will be displayed with an indicator as alert subscription is done with tag name as “subscribed”

All the alerts subscribed for a party will be displayed in the respective categories viz. Current and Savings, Term Deposits, Loans etc. in a table.

To view subscribed alerts for a Party:

6. In the **Group Corporate ID** field, enter the Group Corporate id of the corporate Party.
   OR
   In the **Group Corporate Name** field, enter the name of the Group Corporate.
7. Click **Search**. The Group Corporate id will be displayed based on the search criteria.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to clear the search parameters.

Group Corporate Alerts Subscription - Group Corporate search



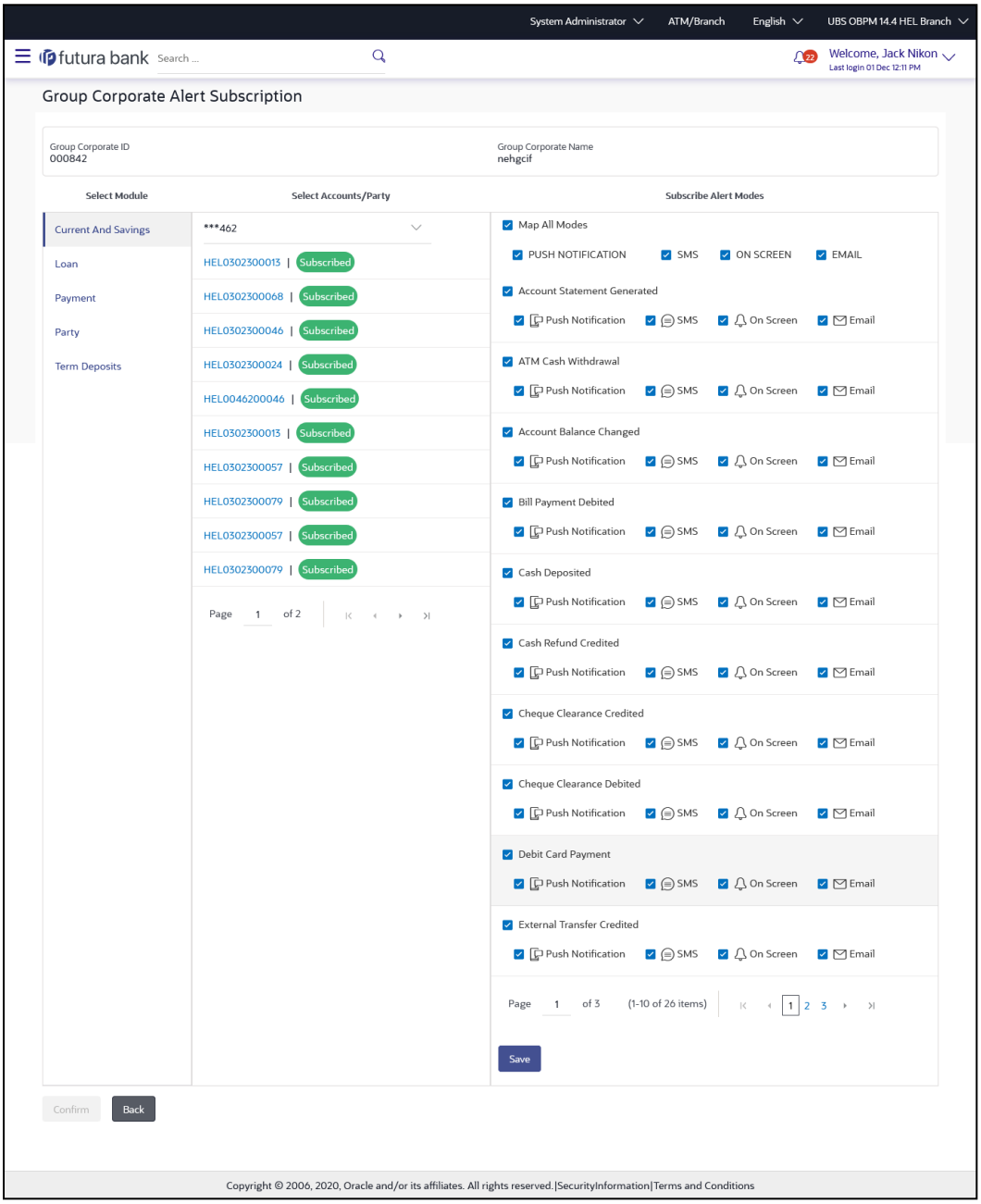
Field Description

Field Name	Description
Group Corporate ID	Enter Group Corporate ID for which the Alerts subscription to be maintained or viewed
Group Corporate Name	Enter Group Corporate name for which the Alerts subscription to be maintained or viewed
Search Result	
Group Corporate ID	Group Corporate ID for which the Alerts subscription to be maintained or viewed
Group Corporate Name	Group Corporate Name for which the Alerts subscription to be maintained or viewed.

8. For the detailed view, click on **Group Corporate ID** field. The tabs for all modules CASA/ Term Deposit/ Loans / Profile that the Group Corporate has access to with the respective Corporate Party associated and account numbers appears.
9. Select the particular Corporate party from the available list and account number to view alert type and delivery mode, for each CASA (Current and Savings Accounts) / TD (Term Deposits) / Loans account.

Note: View the icon on the delivery mode against the alert, if the corporate party has subscribed to any alerts for that.

Group Corporate Alerts Subscription - Detailed View



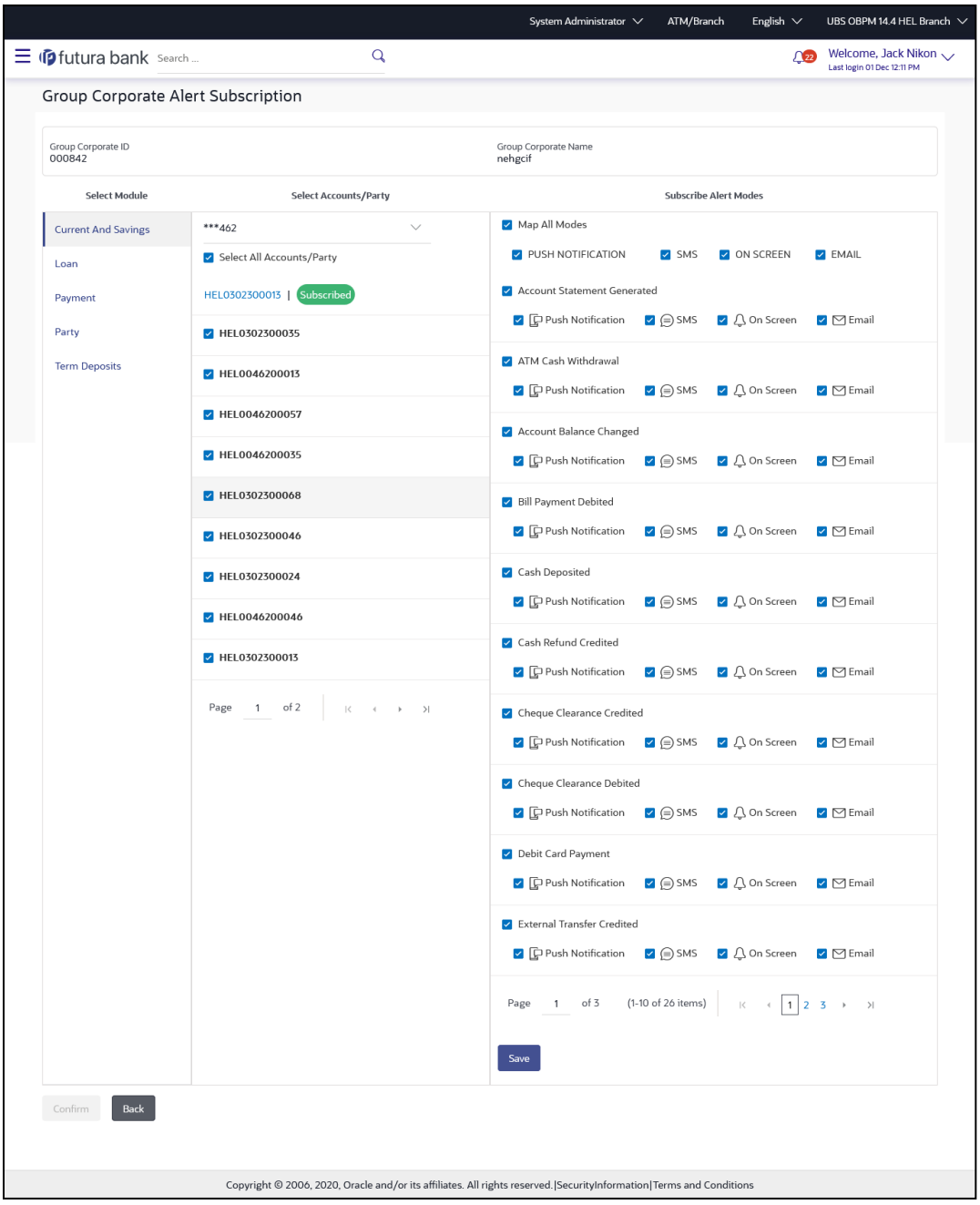
10. Subscribe/ unsubscribe alerts, and click **confirm** to subscribe/ unsubscribe alerts.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to navigate to previous screen.

56.2 Subscribe/ Unsubscribe Alerts

Using this option, Bank Administrator can modify the alerts subscribed for the Corporate Party associated with Group Corporate.

To subscribe / unsubscribe alerts:

11. Repeat steps 1 to 5 of **Alerts Subscription- Search** section.
    The categories viz details of an alert subscribed appears.
12. Select the particular account number to view the alerts subscribed.



Field Description

Field Name	Description
Group Corporate ID	Group Corporate ID for which the Alerts subscription to be maintained.
Group Corporate Name	Group Corporate Name for which the Alerts subscription to be maintained.
Select Party ID	Corporate Party associated with the Group Corporate for whom alerts to be subscribed
Module Name	Name of the module to which alerts is maintained. The options can be: • CASA • Loan • TD • Party • Payments
Account Number	Account number for which the user is viewing/ updating the alert subscription. **Note:** • Bank Admin will be allowed to select and setup alert subscription for multiple or all accounts in single maintenance. • Once the subscription is done for an account that account will be shown with a 'Subscribed' tag.
CASA /TD/ Loans/ Payments	Subscribed alerts displayed in tabs for all modules that the user has access to with the respective account numbers.
Alert Name	The alert type mostly in the form of an event for which an alert is to send to a Corporate Party of Group Corporate.

Field Name	Description
Send Alert Via	The delivery mode through which the alert is to be sent. The options are: • Email: alert is to be sent as an email • SMS : alert is to be sent as an SMS on the Corporate Party of Group Corporates mobile number • On screen Mailbox: on screen, alert sent to as an email to Corporate Party of Group Corporates Mailbox • Push Notification: notifications are sent as a banner or pop-up message on the Corporate Party of Group Corporates mobile number **Note:** The selected mode has icon against it. Bank Admin will be allowed to map all modes of alerts subscription for all the transactions in one go for the selected account

13. Click against the particular account number to update the details.

    b. Click to send alert as an email.
    OR
    Click to send alert as a mail to On screen mailbox.
    OR
    Click to send alert as SMS on the user's mobile number.
    OR
    Click to send alert via push notifications. Push notification is as a banner or pop-up message on the Corporate Party's mobile number.

14. The selected mode has an icon against it.
15. Click **Save** to save the Group Corporate Alert Subscription.
    User will be directed to the Alert Subscription - Edit - Review page post necessary validations.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Back** to go back to previous screen.
16. The **Review** screen appears. Verify the details, and click **Confirm**.
    OR
    Click **Cancel** to cancel the transaction and navigate back to 'Dashboard'.
    OR
    Click **Back** to go back to previous screen.
17. The success message along with the transaction reference number appears. Click **OK to** complete the transaction.

FAQ

1. **Which alerts can the Bank Administrator subscribe or unsubscribe, for the Group Corporate?**

   The alerts, which are not mandatory, can be subscribed or unsubscribed, by the Bank Administrator for the Group Corporate.

2. **What if a Group Corporate wants to opt-out of alerts?**

   The Bank Administrator can unsubscribe the alerts for Group Corporate. Please note that the Corporate will continue to receive the mandatory alerts irrespective of his choice on the subscribed alerts.

3. **Can Bank Administrator subscribe or unsubscribe alert maintenance for multiple corporate parties associated with Group corporate in single flow?**

   Yes. Bank administrator needs to select the corporate party associated with Group Corporate from the available dropdown to subscribe or unsubscribe alert maintenance for multiple corporate parties in single flow.

57. Request Processing

This feature enables the Bank Administrator to view the details of each service request initiated by business user and hence, enables the administrator to take an informed decision regarding the approval or rejection of the service request. Alternately, the administrator can also select multiple service request records from the summary page to approve or reject multiple requests at once. The search criteria provided enables the administrator to filter service requests based on various criteria such as request type, status, reference number, etc.

For the requests built using Service Request Form builder feature, once the Administrator approves/rejects a Service Request, he can change the status of the request and can also enter the comments while updating the status.

Below are the Service Requests that are available out of the box in the system:

- Credit Card Supplementary
- Credit Card PIN Request
- Replace Credit Card
- Update Card Limits
- Update Credit Card Auto Payment
- Register Credit Card Auto Payment
- Deregister Credit Card Auto Payment
- Activate Credit Card
- Hotlist Debit Card
- Cancel Debit Card
- Debit Card PIN Request
- Apply Debit Card
- Replace Debit Card
- Block Debit Card (temporary block)
- Unblock Debit Card (remove temporary block)
- Upgrade Debit Card

Apart from the above mentioned Service Requests, Bank can define new Service Requests definitions using Service Request-Form builder.

Pre-Requisites

- Transaction access is provided to Bank Administrator.

Features Supported In Application

The module supports following features:

- View details of Service Request raised by customers
- Approve / Reject Service Requests
- Changes status of Service Request and input comments (for service requests built using Service Request-form builder)

How to reach here:

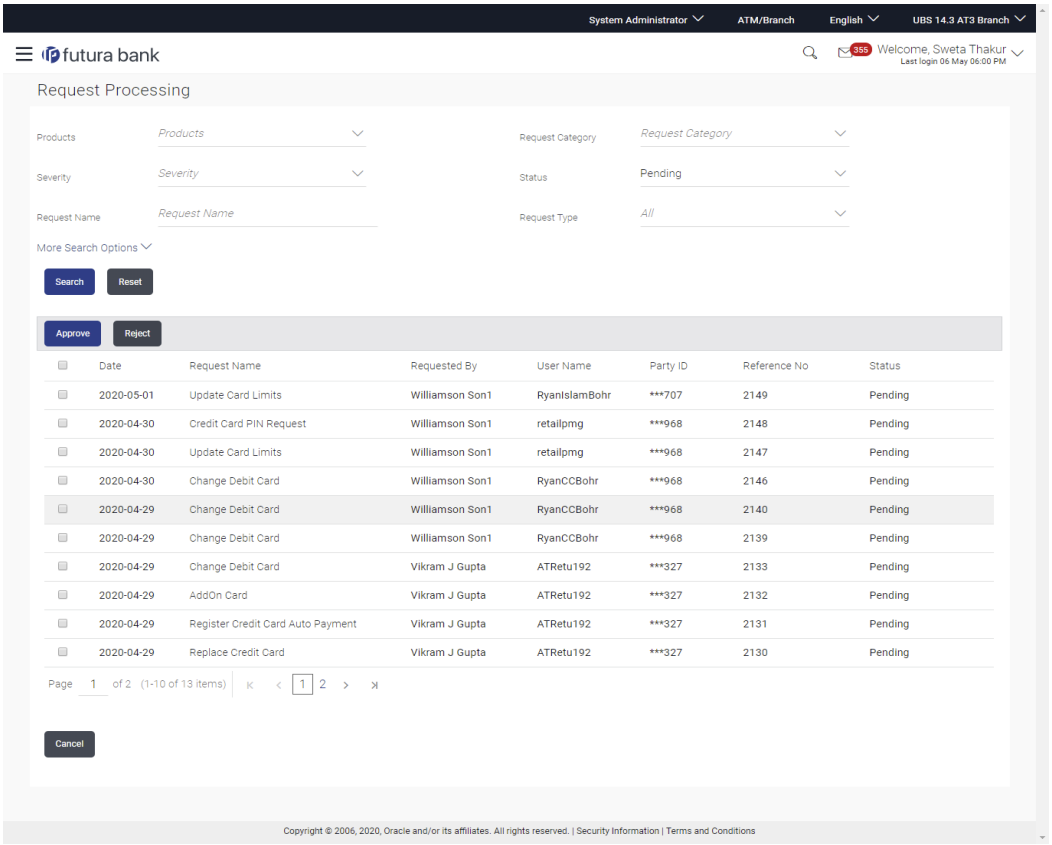
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Others > Request Processing
OR
Bank Administrator Dashboard > Others > Request Processing

57.1 Request Processing - Summary

To view service requests:

1. Select the **Request Processing** option on the dashboard or menu. The initial (summary) page of the Request Processing appears.

Request Processing - Summary



Field Description

Field Name	Description
Search Criteria	
Product	The administrator can search for service requests based on type of product.
Request Category	The administrator can search for service requests based on service request category. Category list gets populated on the basis of the product name selected.
Severity	The administrator can search for service requests based on severity of the service request.
Status	The administrator can search for service requests based on status. On selecting a status, the administrator is required to mandatorily specify a date range so as to be displayed all the service requests that were initiated within the specified date range and that are in the particular status.
Request Name	The administrator can search for service requests on the basis of name of the service request.
Request Type	The administrator can select the type of service request to be displayed in the search result records.
Reference No	The administrator can search for a service request based on reference number that was generated at the time the service request was initiated.
Date Range	The administrator can search for service requests initiated between two dates by specifying a date range. The administrator cannot specify a date range that exceeds 30 days. (The maximum date range is configurable).
First Name	The administrator can search for service requests initiated by a particular business user by specifying the user's first name
Last Name	The administrator can search for service requests initiated by a particular business user by specifying the user's last name or surname
User Name	The administrator can search for service requests initiated by a particular business user by specifying the user's user name.
Party ID	The administrator can search for service requests initiated by business users on the basis of party ID.
Search Results	
Date	The date on which the service request was raised.

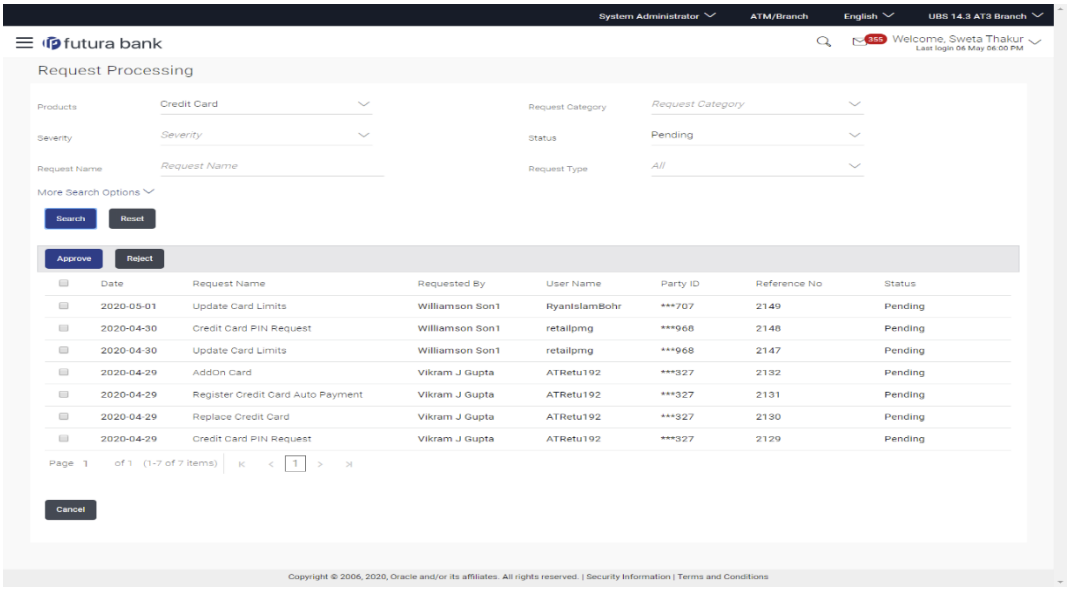
Field Name	Description
Request Name	The name of the service request.
Requested by	The name of the customer who has raised the service request.
User Name	The user name of the customer who has raised the service request
Party ID	The party ID of the user who has raised the service request.
Reference No	The reference number generated at the time the service request was raised.
Status	The current status of the service request.

2. Click on a specific service request record to view the details of that service request.
   OR
   Select the checkbox of one or multiple service requests to approve or reject service requests.

To search for specific service requests:

1. Enter the required information in the search criteria fields.
2. Click **Search**. The specific service request records are displayed based on the search criteria specified.
   OR
   Click **Reset** to clear the search parameters.

Service Request - Search Result



3. Click on a specific service request record to view the details of that service request.
   OR
   Select the check box of one or multiple service requests to approve or reject service requests.

57.2 Service Request Details (For Service Requests available out of the box)

This page is displayed once the Bank Administrator selects a service request record from the previous summary page. This screen comprises of three sections which display the details of the service request, the details of the initiator of the service request and also the transaction journey i.e. a time line graph depicting the stages of the service request.

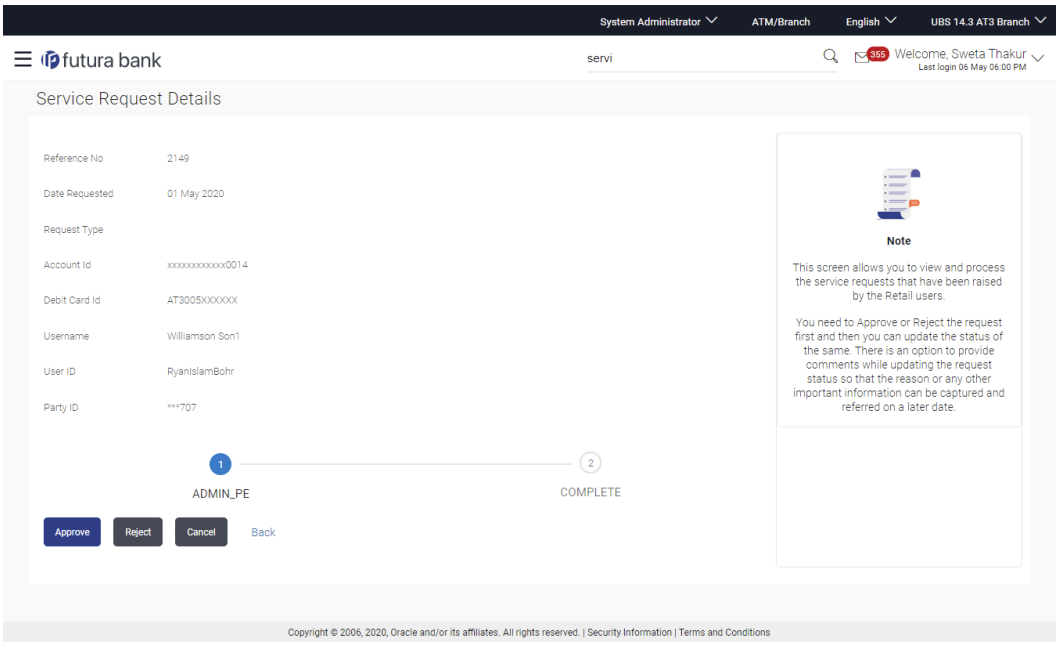
Below are the Service Requests that are available out of the box in the system:

- Credit Card Supplementary
- Credit Card PIN Request
- Replace Credit Card
- Update Card Limits
- Update Credit Card Auto Payment
- Register Credit Card Auto Payment
- Deregister Credit Card Auto Payment
- Activate Credit Card
- Hotlist Debit Card
- Cancel Debit Card
- Debit Card PIN Request
- Apply Debit Card
- Replace Debit Card
- Block Debit Card (temporary block)
- Unblock Debit Card (remove temporary block)
- Upgrade Debit Card

To view the service requests details:

1. Enter the required information in the search criteria fields.
2. Click **Search**. The specific service request records are displayed based on the search criteria specified.
   OR
   Click **Reset** to clear the search parameters.
3. Click on a specific service request record to view the details of that service request. The service request details appears on the **Service Request Details** screen.

Service Request Details



Field Description

Field Name	Description
Request Details	
Reference No	The reference number generated at the time the service request was raised.
Date Requested	The date on which the service request was raised.
Request Type	The type of service request initiated.
User Details	
User Name	The user name of the business user who initiated the service request.

Field Name	Description
User ID	The user Id of the business user who initiated the service request.
Party ID	The party Id of the user who initiated the service request.

Transaction Journey

This section displays the stages of the service request in the form of a timeline graph. Details pertaining to when the service request was initiated along with when the service request was approved or rejected are displayed with the help of this timeline.

4. Click **Approve** to Approve the Service Request.
   OR
   Click **Reject** to Reject the Service Request.
5. Click **Back** to navigate back to the **Request Processing - Summary** screen.

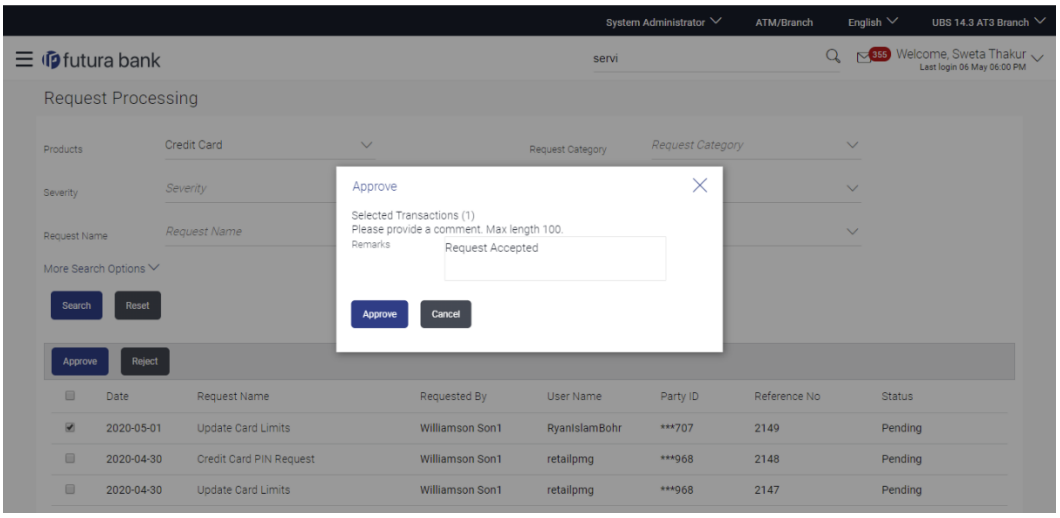
57.2.1 Approve or Reject Service Requests (For Service Requests available out of the box)

The Bank Administrator can take action on service requests initiated by business users by either approving or rejecting requests. The Administrator can select multiple service requests to approve or reject from the Service Request Summary page and can also approve or reject a service request individually after having viewed the details of the request from the Service Request Details page.

To approve / reject service requests from Service Requests Summary page:

1. Select the check boxes of the service requests that you wish to take action on.
   The pop up on which to specify remarks for Approval/Rejection is displayed.
2. Enter **Remarks** and click **Approve**/**Reject**.
   The service requests get approved / rejected.

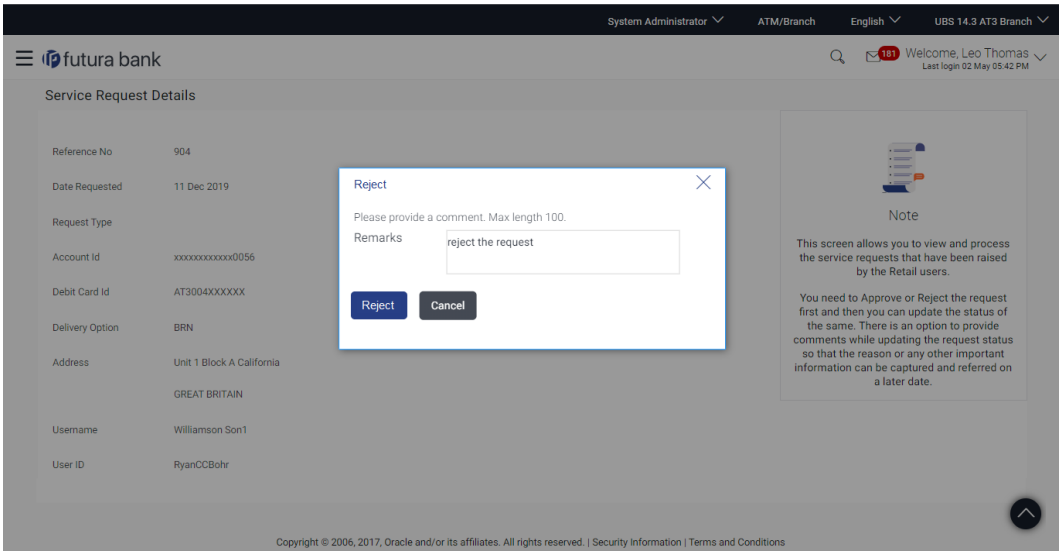
Multiple Service Request Approve or Reject



To approve / reject a service request from the Service Requests Details page:

1. Select the service request on which you wish to take action from the **Service Request** Summary page
2. Click **Approve** or **Reject** button.
   The pop up on which to specify remarks for Approval/Rejection is displayed.
3. Enter Remarks and click **Approve/Reject.**
   The service requests get approved/ rejected.

Individual Service Request Rejection



57.3 Service Request Details (Requests created using Service Request-Form Builder)

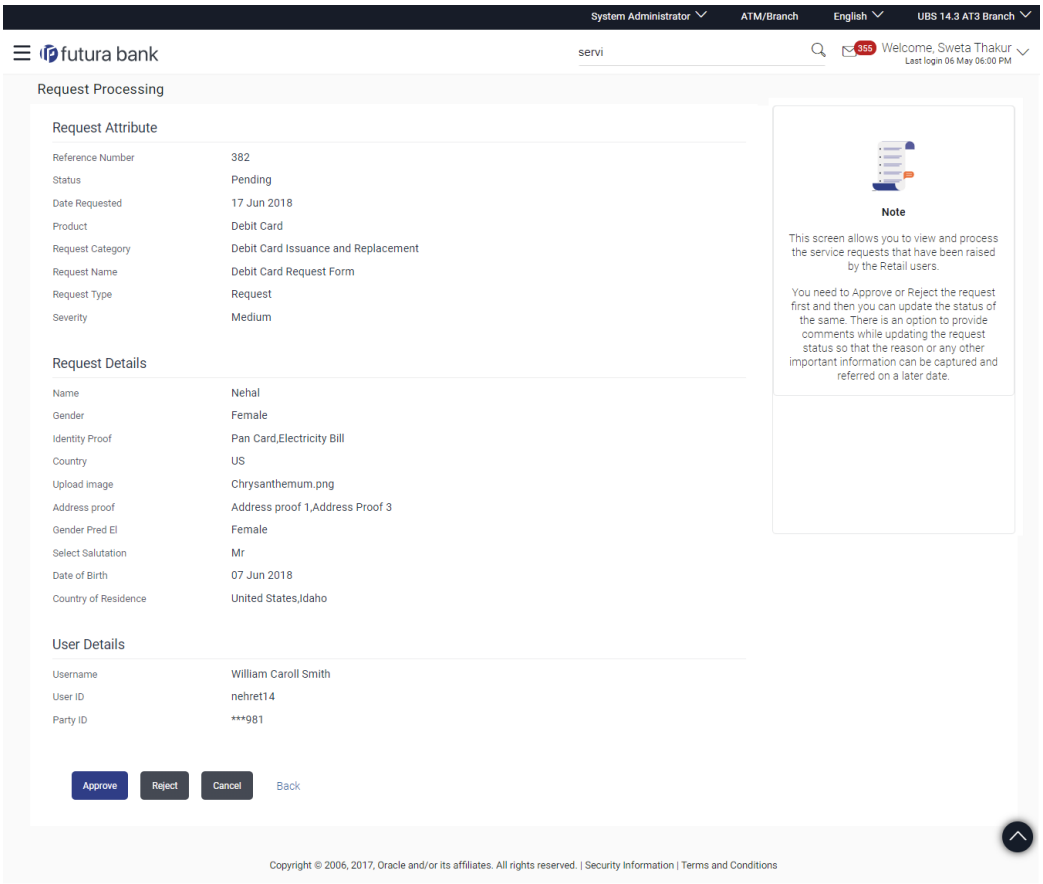
This page appears for the service requests created using ‘Service Request Form Builder’ screen.

The Bank Administrator selects a service request record from the summary page. This screen comprises of three sections which display the request attributes, the details of the service request and the user details.

To view the service requests details:

1. Enter the required information in the search criteria fields.
2. Click **Search**. The specific service request records are displayed based on the search criteria specified.
   OR
   Click **Reset** to clear the search parameters.
3. Click on a specific service request record to view the details of that service request.
   The service request details appears on the **Request Processing** details screen.

Request Processing - Details



Field Description

Field Name	Description
Request Attribute	
Reference No	The reference number generated at the time the service request was raised.
Status	The status of the service request.
Date Requested	The date on which the service request was raised.
Product	The type of product for which the service request was raised.
Request Category	The service request category for which the service request was raised. Category is based on the type of product name selected.
Request Name	The name of the service request.

Field Name	Description
Request Type	The type of service request initiated.
Severity	The severity of the service request.
Request Details	
This section displays the details of the service request. The fields vary depending on the type of service request.	
User Details	
User name	The user name of the business user who initiated the service request.
User ID	The user Id of the business user who initiated the service request.
Party ID	The party Id of the user who initiated the service request.

4. Click **Approve** to Approve the Service Request.
   OR
   Click **Reject** to Reject the Service Request.
5. Click **Back** to navigate back to the **Request Processing - Summary** screen.

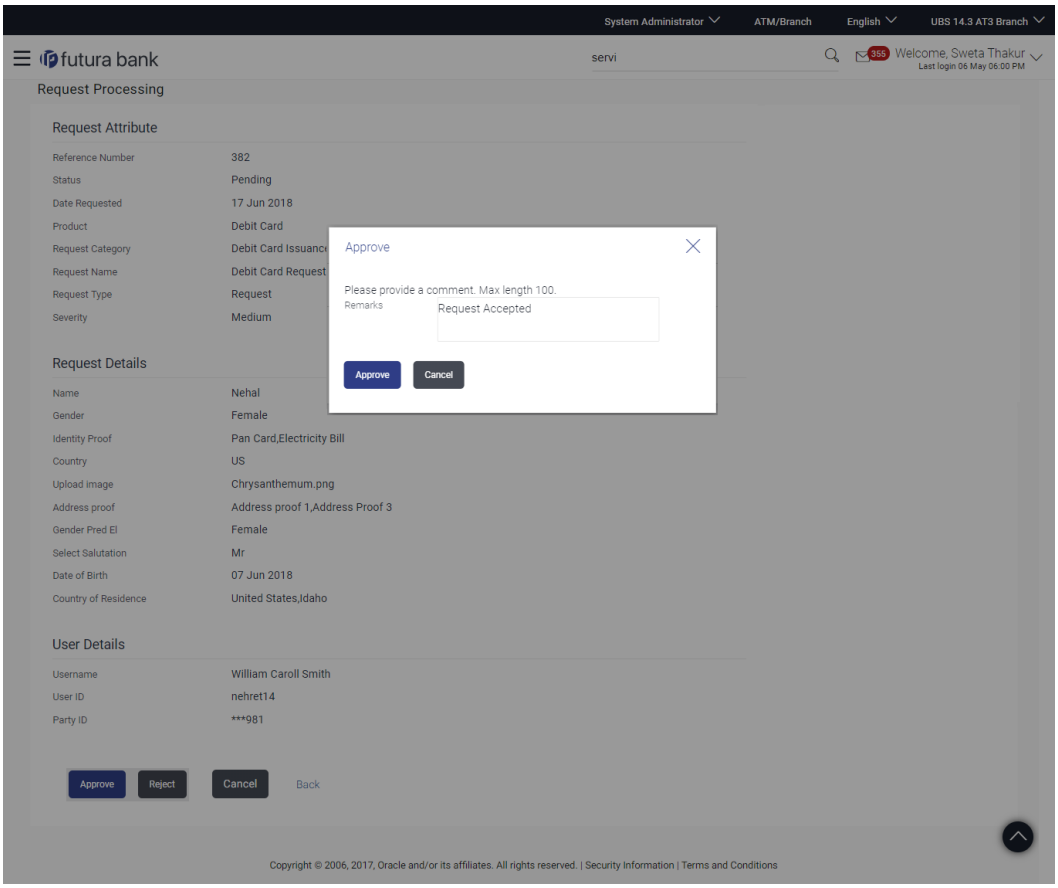
57.3.1 Approve or Reject Service Requests (created using Service Request Form Builder)

The Bank Administrator can take action on service requests initiated by business users by either approving or rejecting requests. The Administrator can select multiple service requests to approve or reject from the Service Request Summary page and can also approve or reject a service request individually after having viewed the details of the request from the Service Request Details page.

To approve / reject a service request:

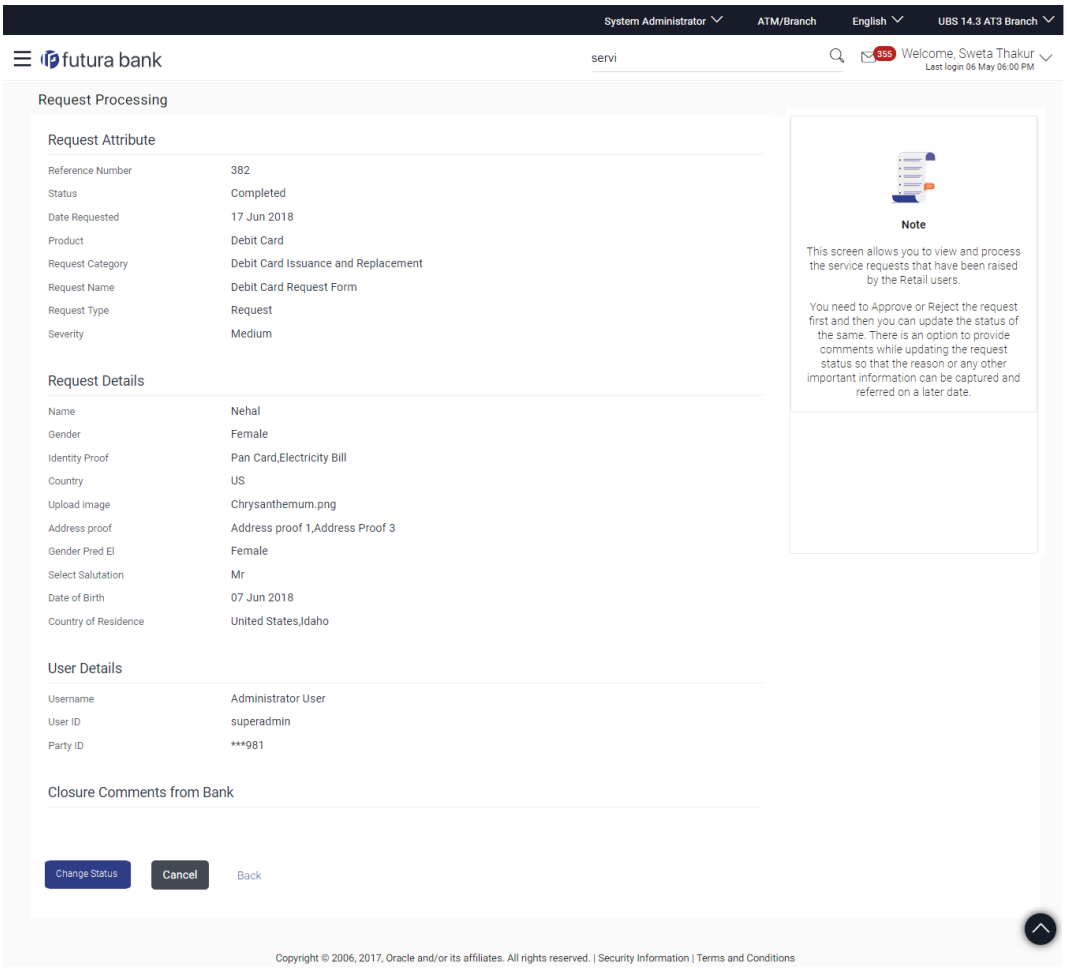
1. Select the service request on which you wish to take action from the **Service Request** Summary page
2. Click **Approve** or **Reject** button.
   The pop up on which to specify remarks for Approval/Rejection is displayed.

Service Request Approval



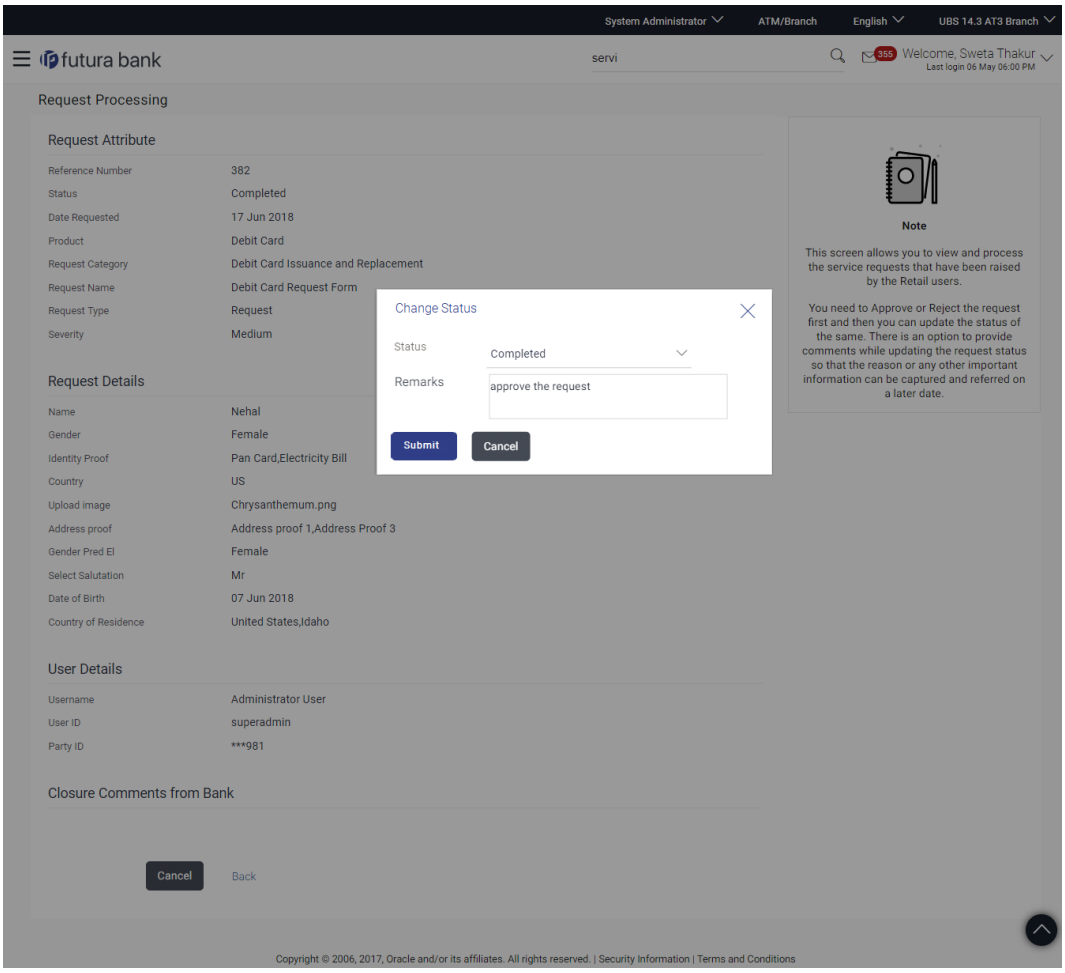
3. Enter Remarks and click **Approve**/**Reject**.
   The success message along with the reference number, service request number and status appears.
4. Click **Ok** to complete the transaction and navigate the dashboard.
5. Navigate to the **Request Processing** transaction and search the service request that you have approved.
   The **Request Processing** details screen appears.

Request Processing - Details



6. Click **Change Status** to change the status of the service request. A pop up to specify remarks appears.
   OR
   Click **Cancel** to cancel the transaction and navigate to the dashboard.
   OR
   Click **Back** to navigate to previous screen.

Request Processing - Change Status



Field Description

Field Name	Description
Change Status	
Status	The status of the service request.
Remarks	Remarks for changing the status of the service request.

7. From the **Status** list, select the status of the service request.
8. In the **Remarks** field, enter the remarks if any.
9. Click **Submit**.
   The success message along with the reference number, service request number and status appears.

58. Terms and Conditions Maintenance

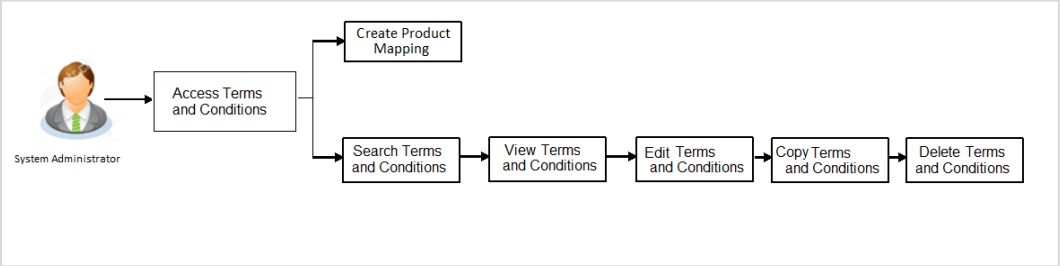
Terms and Conditions are set by Bank to layout the expected guidelines, and act as the backbone for the transactional agreement between customer and the bank.

Terms and Conditions Maintenance screen allows the bank administrator user to maintain terms and condition text for All/Specific Parties for All/Specific Transactions, so that corporate users gets to view and accept it while initiating a trade finance transaction.

Pre-Requisites

- Transaction access is provided to Bank Administrator.
- Approval rule set up for Bank Administrator to perform the actions.
- Party for which preference needs to be set up is created in core banking application.

Workflow



Features Supported In Application

Terms and Conditions maintenance available for bank administrator in the application includes:

- Create Terms and Conditions
- View Terms and Conditions
- Edit Terms and Conditions
- Delete Terms and Conditions
- Copy Terms and Conditions

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu> Menu > Others > Terms and Conditions Maintenance

58.1 Terms and Conditions - Search and View

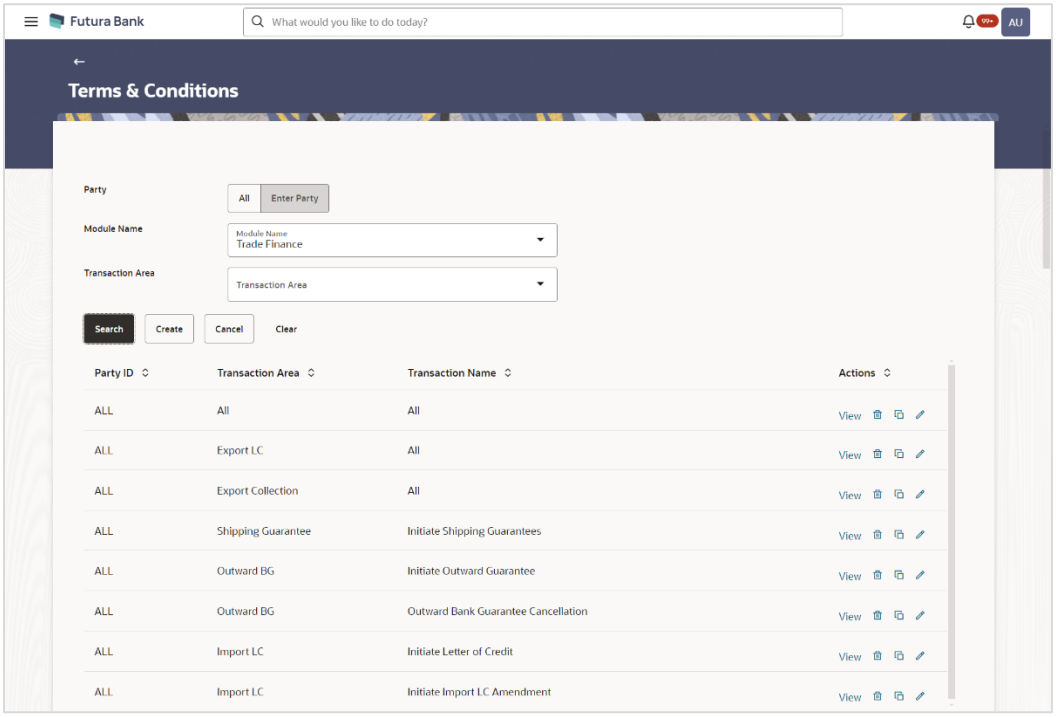
Bank Administrator can search and view the previously maintained Terms and Conditions. Administrator can narrow the result using the available fields as filters such as ALL or Specific Party ID, Module, Transaction Area and Transaction Name (Only If he selects any Specific Transaction Area).

All the applicable transactions will be listed here, and user can select any maintenances from the list, by clicking on view to see the details.

To search Terms and Conditions:

1. In the **Party** field, select the appropriate tab.

Terms and Conditions - Search and View



Field Description

Field Name	Description
Party	Option to select the party type. The options are: • All • Enter Party
Party ID	Party ID for which the term and conditions are maintained/ viewed. This field appears if **Enter Party** option is selected in the **Party** field.
Module Name	The name of the module. Only Trade Finance is supported.
Transaction Area	The list of transaction area which are a part of transaction group.

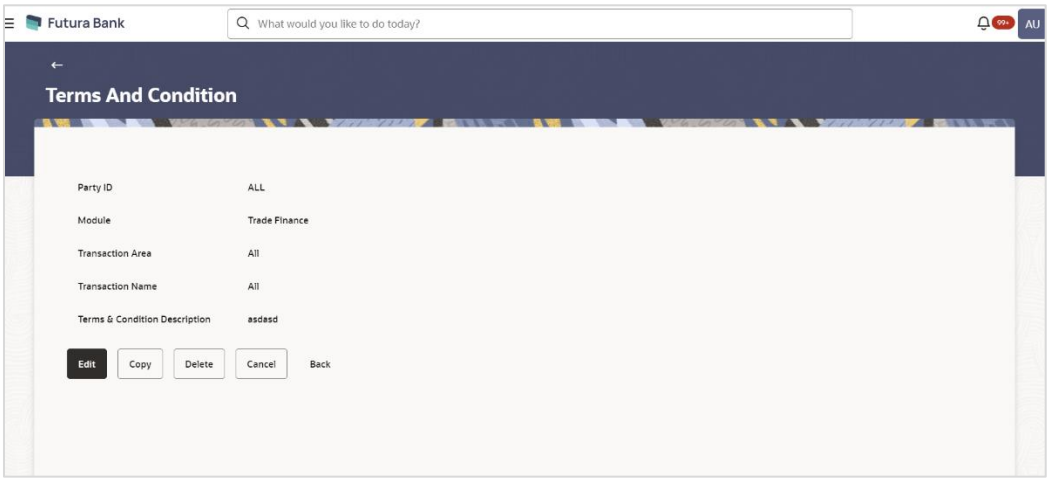
Field Name	Description
Transaction Name	Name of transactions which are a part of transaction group. This field appears if any transaction other than **All** is selected in the **Transaction Area** list.
Search Result	
Party ID	Party ID for which the term and conditions are maintained/ viewed.
Transaction Area	The list of transaction groups of Trade Finance Module.
Transaction Name	Name of transactions which are a part of transaction group. This field appears if any transaction other than **All** is selected in the **Transaction Area** list.
Actions	The available actions that can be performed against the term and conditions for transactions are displayed. The actions can be: • View: Click to view the already maintained terms and conditions. • Delete ( ): Click to delete the already maintained terms and conditions. • Copy ( ): Click to copy the already maintained terms and conditions. • Edit ( ): Click to edit the already maintained terms and conditions.

2. If you have selected **Enter Party** option, specify the party ID in the **Party ID** field.
3. From the **Transaction Area** list, select the appropriate option.
4. From the **Module Name** list, select the listed option.
5. If you have selected any transaction other than **All**;
6. From the **Transaction Name** list, select the appropriate transaction.
7. Click **Search**. The screen displays results based on search criteria.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
   OR
   Click **Clear** to reset the details.

58.1.1 Terms and Conditions - View

8. In the Terms and Conditions search result screen, click the **View** link to view the already maintained terms and conditions.

Terms and Conditions - View



Field Description

Field Name	Description
Party ID	Party ID for which the term and conditions are maintained/ viewed.
Module Name	The name of the module. Only Trade Finance is supported.
Transaction Area	The list of transaction area which are a part of transaction group.
Transaction Name	Name of transactions.
Terms & Conditions Description	The description of already maintained terms and conditions.

9. Click **Edit** to edit the Terms & Conditions description.
   OR
   Click **Copy** to copy the Terms & Conditions text.
   OR
   Click **Delete** to delete the Terms & Conditions description.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.

58.2 Create Terms and Conditions

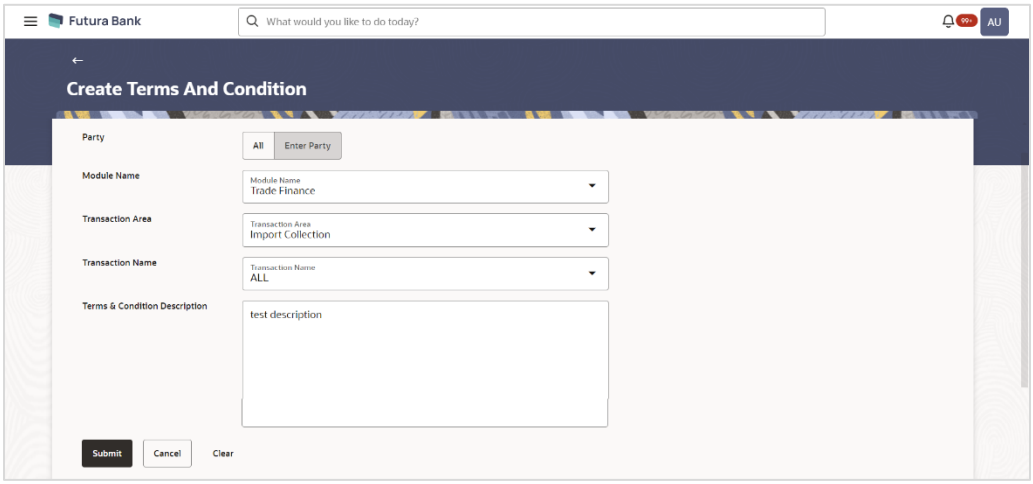
Using this option, Bank Administrator can configure terms and conditions for a specific party. The administrator user can select the maintenance for all parties or for a specific party. The administrator user can also select the term and condition text to appear for all transactions or specific ones.

Admin will get a list of transactions areas, which are high level classification. Under each Transaction area, there can be several Transactions names which are the actual transactions getting initiated at OBDX. Admin user can select one of them, or all and have the Terms and Condition maintained for it.

To create Terms and Conditions text:

1. In the **Terms and Conditions** screen, click **Create Terms & Conditions**.
   The **Create Terms and Conditions** screen appears.

Create Terms and Conditions



Field Description

Field Name	Description
Party	Option to select the party type. The options are: • All • Enter Party
Party ID	Party ID for which the term and conditions are maintained/ viewed. This field appears if **Enter Party** option is selected in the **Party** field.
Module Name	The name of the module. Only Trade Finance is supported currently.
Transaction Area	The list of transaction area which are a part of transaction group.

Field Name	Description
Transaction Name	Name of transactions which are a part of transaction group. This field appears if any transaction other than **All** is selected in the **Transaction Area** list.
Terms & Conditions Description	The description of terms and conditions that is to be created.

2. If you have selected **Enter Party** option, specify the party ID in the **Party ID** field.
3. From the **Transaction Area** list, select the appropriate option.
4. From the **Module Name** list, select the listed option.
5. If you have selected any transaction other than **All**;
6. From the **Transaction Name** list, select the appropriate transaction.
7. In the **Terms & Conditions Description** field, enter the description terms and conditions.
8. Click **Submit**. The screen displays results based on search criteria.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
   OR
   Click **Clear** to reset the details.
9. The **Review Terms and Conditions** screen appears. Verify the details and click **Submit**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.
10. The success message appears along with the transaction reference number and status. Click **OK** to complete the transaction and navigate back to 'Dashboard'.

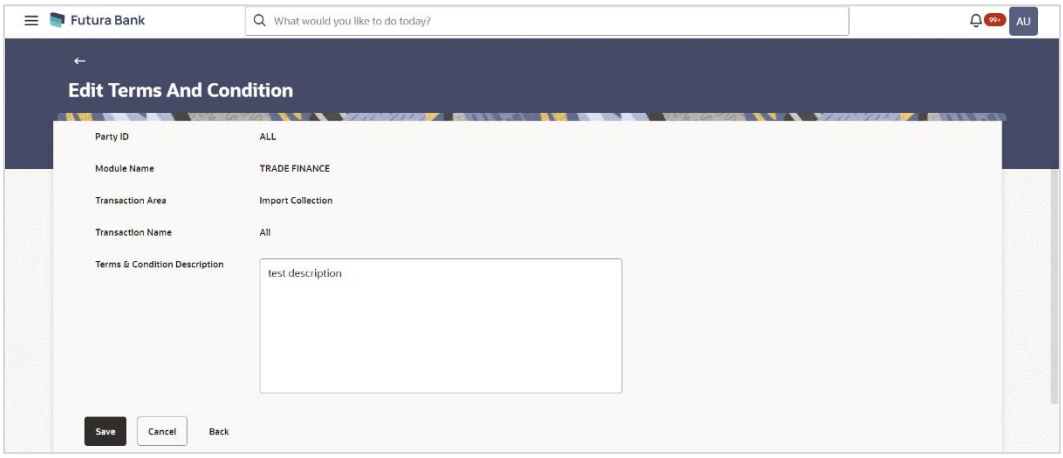
58.3 Edit Terms and Conditions

Administrator can edit the party terms and conditions description.

To edit the terms and conditions description:

1. In the **Terms and Conditions** search result screen, click the icon to view the already maintained terms and condition description.
   OR
   In the **Terms and Conditions View** screen, click **Edit** to edit the already maintained terms and condition description.
   The **Edit Terms and Conditions** screen appears.

Edit Terms and Conditions



2. In the **Terms & Conditions Description** field, modify the description of terms and conditions, if required.
3. Click Submit. The screen displays results based on search criteria.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
   OR
   Click **Clear** to reset the details.
4. The **Review** Terms and Conditions screen appears. Verify the details and click **Submit**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.
   OR
   Click **Back** to navigate to the previous screen.
5. The success message appears along with the transaction reference number and status. Click **OK** to complete the transaction and navigate back to 'Dashboard'.

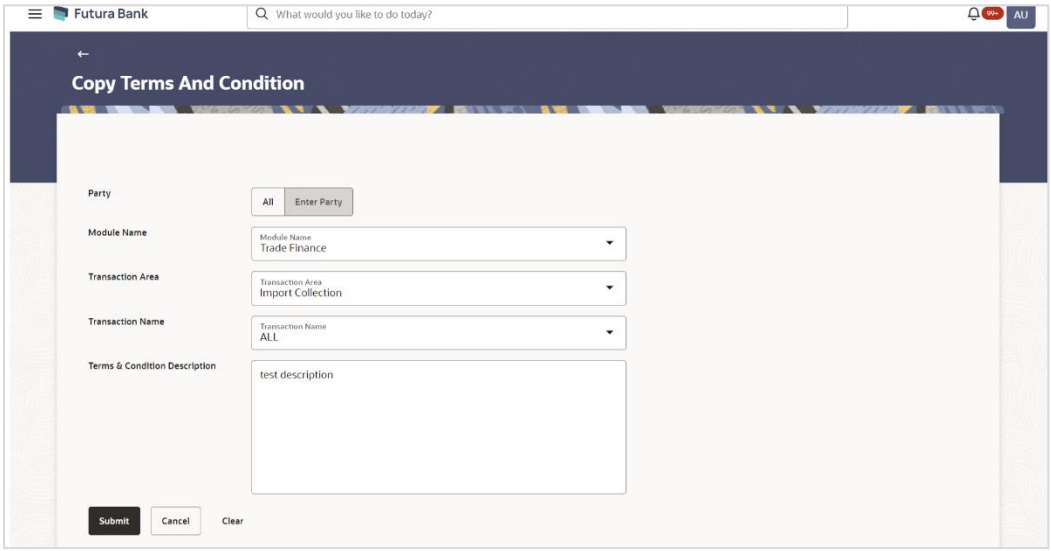
58.4 Copy Terms and Conditions

Administrator can copy the already maintained terms and conditions description.

To copy the terms and conditions description:

1. In the **Terms and Conditions** search result screen, click the icon to copy the already maintained terms and condition description.
   OR
   In the **Terms and Conditions View** screen, click **Copy** to copy the already maintained terms and condition description.
   The **Copy Terms and Conditions** screen appears.

Copy Terms and Conditions



Field Description

Field Name	Description
Party	Option to select the party type. The options are: • All • Enter Party
Party ID	Party ID for which the term and conditions are maintained/ viewed.
Module Name	The name of the module. Only Trade Finance is supported.
Transaction Area	The list of transaction area which are a part of transaction group.
Transaction Name	Name of transactions.
Terms & Conditions Description	The description of already maintained terms and conditions.

2. In the **Terms & Conditions Description** field, copy the description of terms and conditions.
3. Click Submit. The screen displays results based on search criteria.
   OR
   Click **Cancel** to cancel the transaction and navigate the user back to **Dashboard**.
   OR
   Click **Clear** to reset the details.
4. The **Review** Terms and Conditions screen appears. Verify the details and click **Submit**.
   OR
   Click **Cancel** to cancel the operation and navigate back to 'Dashboard'.

OR
Click **Back** to navigate to the previous screen.

5. The success message appears along with the transaction reference number and status. Click **OK** to complete the transaction and navigate back to ‘Dashboard’.

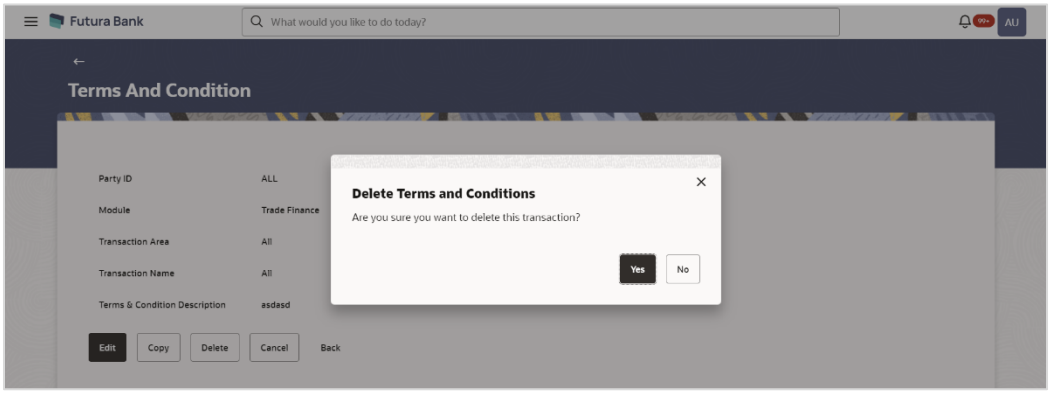
58.5 Delete Terms and Conditions

Administrator can delete the terms and conditions description.

To delete the terms and conditions description:

1. In the **Terms and Conditions** search result screen, click the icon to delete the already maintained terms and condition.
   OR
   In the **Terms and Conditions View** screen, click the **Delete** to delete the already maintained terms and condition.
   The application will prompt the administrator with a deletion message.

Delete Terms and Conditions



2. Click **Yes** to proceed with the deletion request. It will navigate to confirmation page with a success message and the status.
3. Click **Ok** to close the screen and navigate to the dashboard.

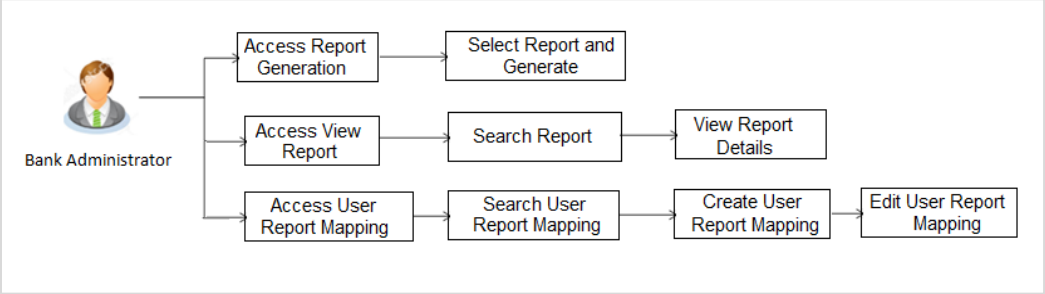
59. Reports

Using this option, Administrators can generate various adhoc and schedule banking reports. Application provides an option to generate and schedule reports using Oracle Analytics Publisher Oracle Analytics and also by using an internal application. The adoption Oracle Analytics Publisher provides a simple and easy tool for the Operational and MIS reports

Prerequisites:

- Transaction access is provided to Bank Administrator
- Approval rule set up for Bank Administrator to perform the actions.
- Oracle Analytics Publisher is configured.

Workflow



Features supported in application

Reports module allows Bank Administrator to

- Generate and schedule Customer and Administrative Reports
- View/ Download generated Reports.
- View User Report Mapping
- Create User Report Mapping
- Edit User Report Mapping
- View Scheduled Report

60. Report Generation

Bank Administrator logs into the system and navigates to Report Generation screen. On accessing 'Report Generation menu, Bank Administrator has to select an option if an adhoc report is to be generated or report needs to be scheduled.

Reports are categorized as:

- Adhoc Reports: When a report needs to be generated immediately on a need basis
- Schedule Reports: When report generation needs to be scheduled at fixed intervals e.g. daily, weekly, monthly etc.

After selecting the report generation category, user has to select a type of a report which needs to be generated. Other reports parameters with respect to each report are displayed on the screen as input fields so that report can be requested with specific data.

Note: If 2 factor authentication is enabled, the reports get generated only after successful authentication.

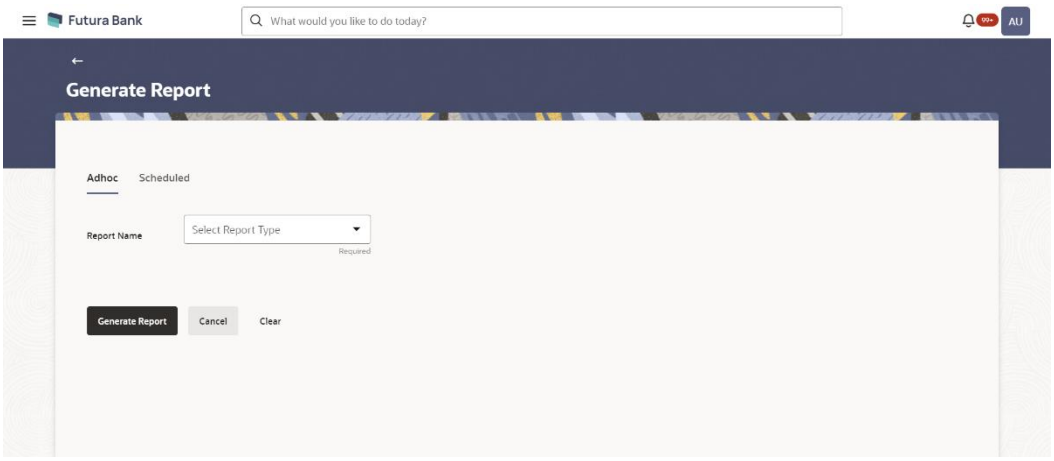
The list of reports is:

- API Consumption Report
-
- Date wise User Creation Report
- EPI Payment reconciliation Report
- FATCA &CRS Declaration Report
- File Identifier wise Party User Mapping Report
- Party User wise File Identifiers Mapping Report
- Approval Rule Report
- Party wise File Identifiers Mapping Report
- Party wise Payee Maintenance Report
- User Segment Summary Report
- User List Report
  - User Entitlement Report
  - Approval Rule Report

How to reach here:

System/ Bank Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

Report Generation



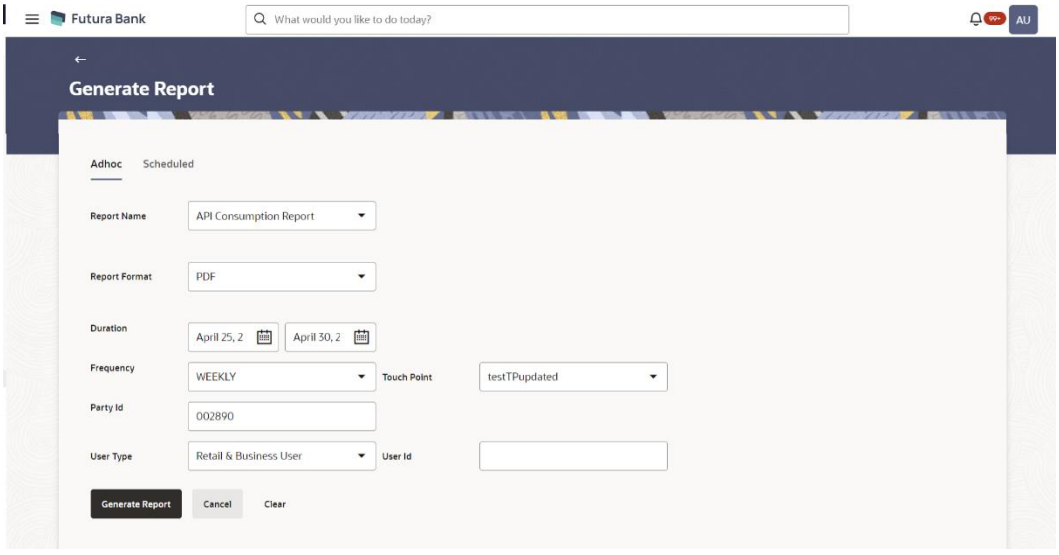
Field Description

Field Name	Description
Report Name	Select the type of report to be generated.

60.1 Adhoc Reports

Adhoc reports are generated on demand or on request. Generated reports can be viewed using ‘My Reports’ screen.

Adhoc Reports



Field Description

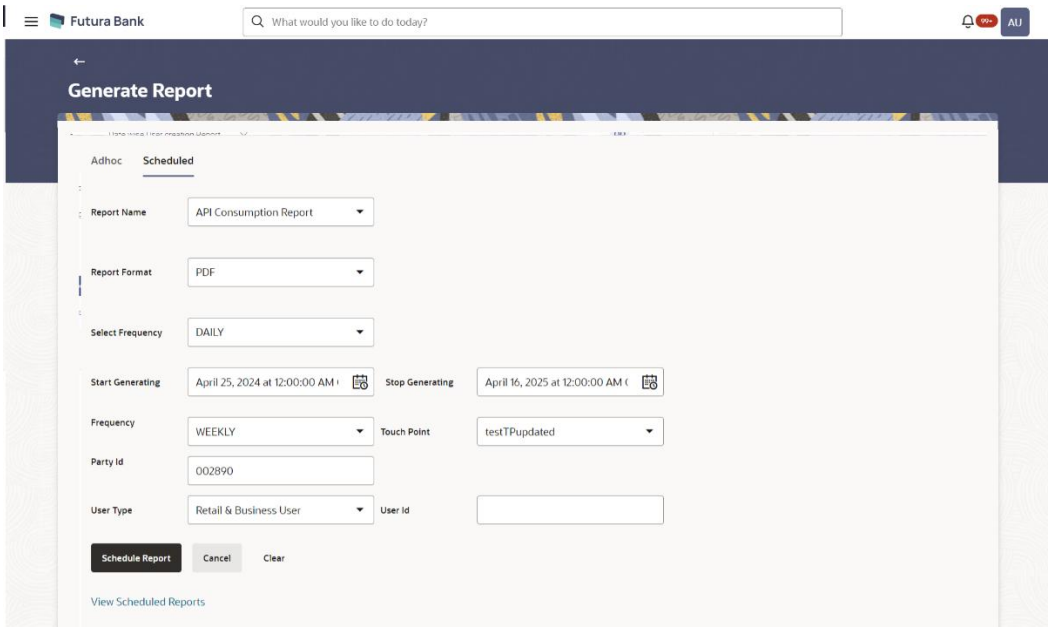
Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated. The options with Oracle Analytics PublisherOracle Analytics are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV

Note: Other reports parameters with respect to each report are displayed on the screen as input fields so that report can be requested with specific data.

60.2 Schedule Reports

The reports that are generated in specific time frame such as daily, weekly, monthly, quarterly, and annually are categorized under scheduled reports.

Schedule Reports



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated. The options with Oracle Analytics PublisherOracle Analytics are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV
Select Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly
Start Generating	Start date of the date range from which you want to generate the report.
Stop Generating	End date of the date range up-to which you want to generate the report.
View Scheduled Reports	Link to view all the reports that are scheduled by the logged in user and other Bank administrator users.

Note: Other reports parameters with respect to each report are displayed on the screen as input fields so that report can be requested with specific data.

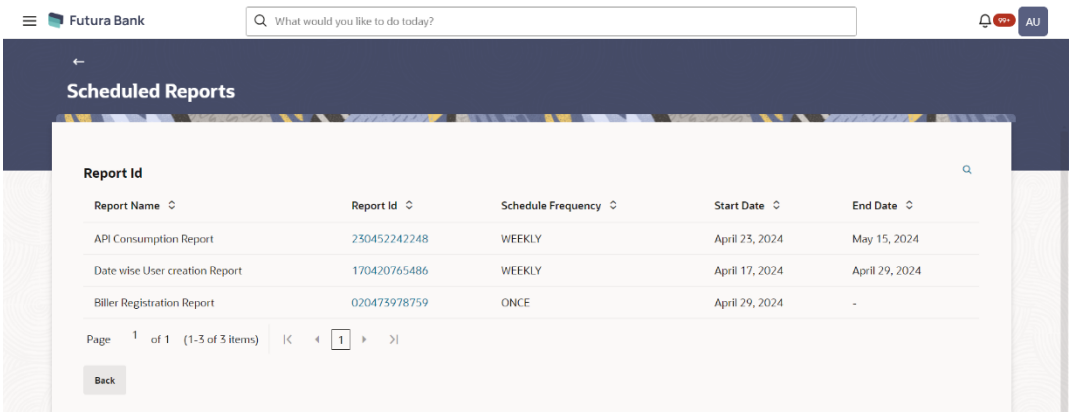
60.2.1 View Scheduled Reports

Using this option, Bank Administrator can view all the reports and its details that are scheduled by logged in user or any other Bank Administrator user with the future date.

To view the scheduled reports:

1. Click the **Schedule** tab. The scheduled report generation screen appears.
2. Click the **View Scheduled Reports** link.
   The **Scheduled Reports** screen appears.

Scheduled Reports

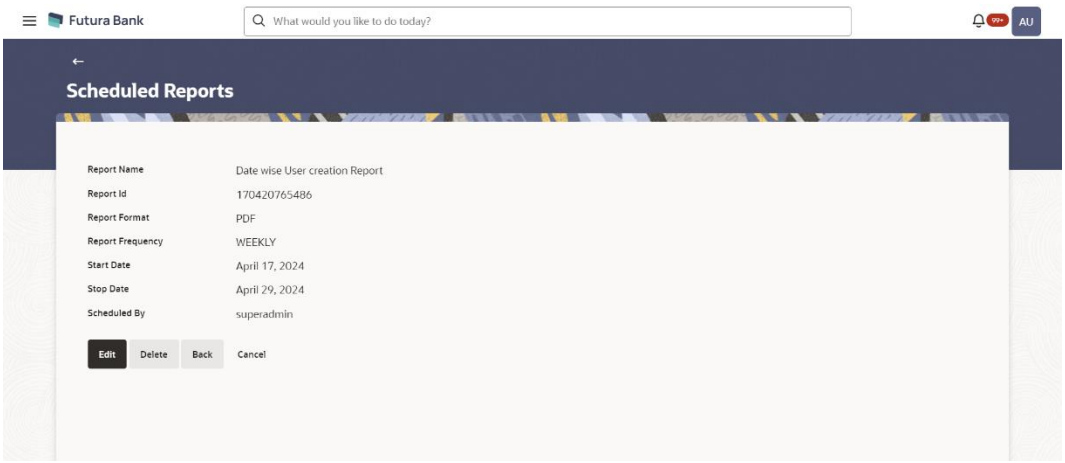


Field Description

Field Name	Description
Search	
Report Name	Select the report that is to be searched.
Search Results	
Report Name	Name of the scheduled reports.
Report ID	IDs of the reports that are scheduled.
Schedule Frequency	The frequency on which the report is scheduled.
Start Date	Date from which the report will be generated as per the frequency defined.
End Date	Date till which the report will be generated as per the frequency defined.

3. Click on desired **Report ID** to view the details of the scheduled report. The **View Reports Schedule** screen appears.
   OR
   Click on the icon against the Report ID, to select the **Report from the** list, which you want to view. The searched report appears in the search result section.
   Click the **Report ID** to view the details of the scheduled report.

View Reports Schedule



Field Description

Field Name	Description
Report Name	Name of the scheduled report.
Report ID	ID of the scheduled report.
Report Format	Select the format in which the report is to be generated.
Report Frequency	The frequency at which the reports are scheduled to run.
Start Date	Date from which the report will be generated as per the frequency defined.
Stop Date	Date till which the report will be generated as per the frequency defined.
Scheduled By	User ID of the user who has scheduled the report generation.

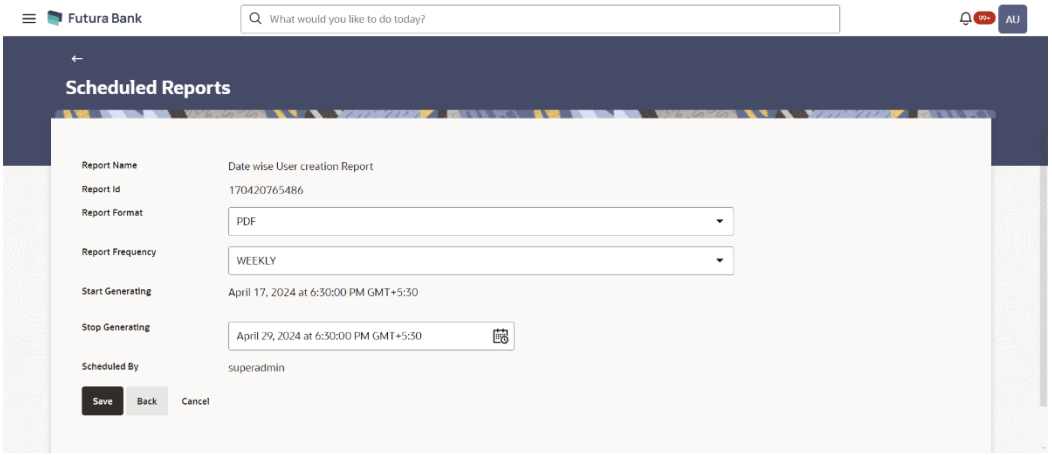
60.2.2 Edit Schedule Reports

Using this option, Bank Administrator can edit the parameters defined for scheduled reports. These changes are applied to generate the reports of next scheduled cycle.

To edit the schedule reports:

1. Click the **Schedule** tab. The scheduled report generation screen appears.
2. Click the **View Scheduled Reports** link.
   The **Scheduled Reports** screen appears.
3. Click on desired **Report ID** to edit the details of the scheduled report. The **View Report Schedule** screen appears.
4. Click **Edit** to modify the report schedule. The **Edit Report Schedule** screen appears.
   OR
   Click **Delete** to delete the report schedule.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.

Edit Reports Schedule



Field Description

Field Name	Description
Report Name	Name of the scheduled reports. Name of the report will be displayed in non-editable form.
Report ID	ID of the reports that are scheduled. This is a non-editable field.
Report Format	The report format of the scheduled report.

Field Name	Description
Report Frequency	The frequency of the scheduled report. The options are: • Once • Daily • Weekly • Monthly
Start Generating	The start date of the scheduled report. This field can be edited only if the date and time is in future.
Stop Generating	The date till which the report is to be generated.
Scheduled By	User ID of the user who scheduled the report generation.

5. Modify the details, if required. You can modify the Report Format, Report Frequency, Start generation date and time (if future date) and Stop Generating date and time.
6. Click **Save** to save the changes. The **Confirm Edit Report Schedule** screen appears.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.
7. Click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
8. The success message along with the reference number and status appears.
   Click **Ok** to close the screen and navigate to the dashboard.

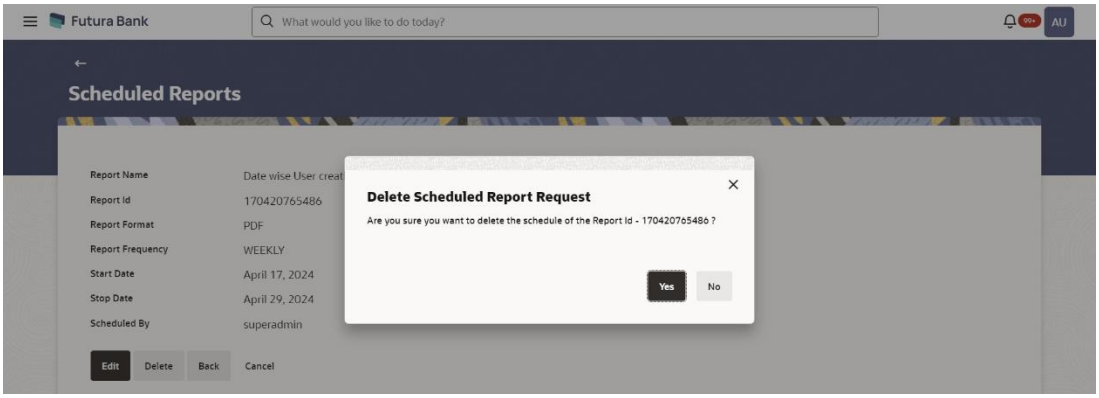
60.2.3 Delete Schedule Reports

The Bank Administrator can delete the scheduled reports which are no longer required.

To delete account and transaction access for the user:

1. In the **Reports** screen, click the **Schedule** tab. The scheduled report generation screen appears.
2. Click the **View Scheduled Reports** link.
   The **Schedule Reports** screen appears.
3. Click on desired **Report ID** to delete the scheduled report. The **View Report Schedule** screen appears.
4. Click **Delete**.
   The application will prompt the administrator with a deletion message.

Delete Reports Schedule



5. Click **Confirm** to proceed with the deletion request. It will navigate to confirmation page with a success message and the status.
6. Click **Ok** to close the screen and navigate to the dashboard.

60.3 API Consumption Report

API Consumption report provides information on API consumption for a selected access point for a particular user.

The user has to select a format in which the report needs to be generated. The generation of both Adhoc and Scheduled reports are supported.

How to reach here:

Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

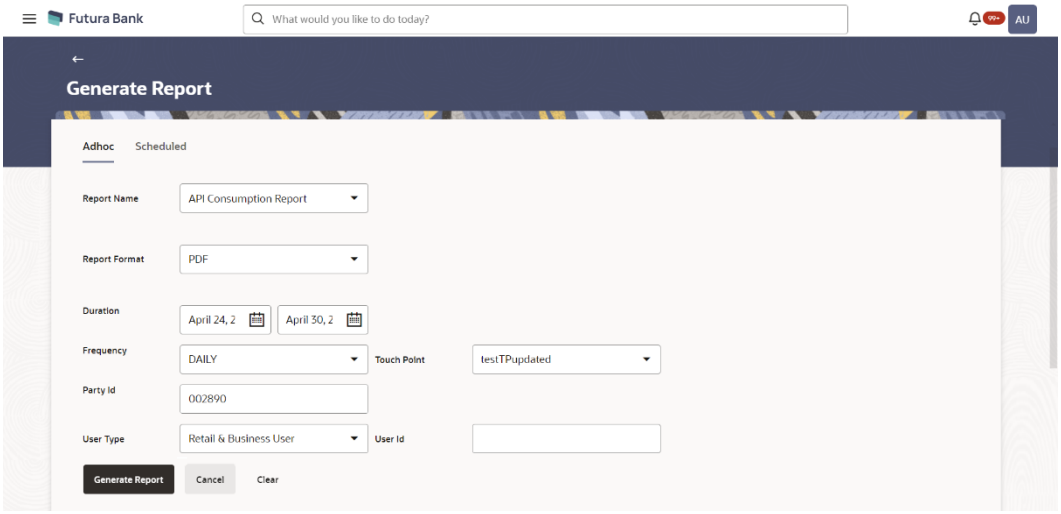
60.3.1 API Consumption - Adhoc Report

API Consumption Adhoc report is generated on demand or on request. Report can be requested from the 'Report Generation' screen. Adhoc reports can be viewed using 'My Reports' screen.

To generate the API Consumption adhoc report:

1. Click the **Adhoc** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The respective report generation screen appears.

API Consumption - Adhoc Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated The options with Oracle Analytics PublisherOracle Analytics are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV
Duration	The period for which the report is to be generated. Start date of the date range from which you want to generate the report. End date of the date range up-to which you want to generate the report.
Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly
Touch Point	The different channels/ medium for which you want to generate the report.
Party ID	The party ID for whom the report is to be generated.
User Segment	The segment of user for whom the report is to be generated. The options are: • Corporate User • Retail User • Administrator
User id	The user id of the user for whom the report is to be generated.

3. From the **Report Format** list, select the appropriate report output format.
4. From the **Duration - From Date** and **Duration - To Date** list, select the appropriate duration.
5. From the **Frequency** list, select the appropriate option.
6. From the **Touch Point** list, select the appropriate option.
7. In the **Party ID** field, enter the party id.

8. From the **User Segment** list, select the appropriate type of user.
9. In the **User Id** field, enter the id of the user for whom the report is to be generated.
10. Click **Generate Report** to generate the report.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Clear** to reset the search parameters.
11. The success message along with the reference number, status and **Report Request Id** appears. Click **Ok** to close the screen and navigate to the dashboard.
    OR
    Click on the **View Reports** link to download the report. The user is directed to the **My Reports** screen. The list of reports appears.
    OR
    Click **Generate another report** to generate another report.
12. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated is given below:

API Consumption Details Report

futura bank

From Date : **2018-10-12** | To Date : **2018-11-12**
Frequency : **WEEKLY** | Touch Point : **APINTERNET**
Party Id : | Party Name :
User Segment : | User Id :

API Name	/accessPointGroups			
From Date	To Date	Count:	Touch Point	Status
29-OCT-2018	05-NOV-2018	919	APINTERNET	Success Count: 906Failure Count:13

API Name	/accessPointGroups/{accessPointGroupId}			
From Date	To Date	Count:	Touch Point	Status
29-OCT-2018	05-NOV-2018	1	APINTERNET	Success Count: 1Failure Count:0

API Name	/accessPointScopes			
From Date	To Date	Count:	Touch Point	Status
29-OCT-2018	05-NOV-2018	42	APINTERNET	Success Count: 42Failure Count:0

API Name	/accessPoints			
From Date	To Date	Count:	Touch Point	Status
29-OCT-2018	05-NOV-2018	2872	APINTERNET	Success Count: 2857Failure Count:15

API Name	/accessPoints/{accessPointId}			
From Date	To Date	Count:	Touch Point	Status
29-OCT-2018	05-NOV-2018	42	APINTERNET	Success Count: 42Failure Count:0

API Name	/accesstokens			
From Date	To Date	Count:	Touch Point	Status
29-OCT-2018	05-NOV-2018	2823	APINTERNET	Success Count: 2821Failure Count:2

API Name	/accesstokens/{id}			
From Date	To Date	Count:	Touch Point	Status
29-OCT-2018	05-NOV-2018	2	APINTERNET	Success Count: 2Failure Count:0

API Name	/accesstokens/{stateId}/{code}			
From Date	To Date	Count:	Touch Point	Status
29-OCT-2018	05-NOV-2018	11	APINTERNET	Success Count: 6Failure Count:5

API Name	/accountAccess			
From Date	To Date	Count:	Touch Point	Status
29-OCT-2018	05-NOV-2018	752	APINTERNET	Success Count: 723Failure Count:29

1 Report generated by superadmin | 14 Nov 2018, 08:03

Field Description

Field Name	Description
Report Parameters	
From Date	Date from which the report is generated.
To Date	Date till which the report is generated.
Frequency	The frequency at which the report is generated.
Access Point (Touch Point)	The different channels/ medium for which report is generated.
Party ID	The party ID for whom the report is generated.
Party Name	The name of the party for whom the report is generated.
User Segment	The user segment for which, the report is generated.
User ID	ID of the user.
API Name	The name of the API for which the report is generated.
From Date	Date from which the report is generated.
To Date	Date till which the report is generated.
Count	The total count of transactions that are successful and failed.
Touch Point	The different channels/ medium for which report is generated.
Status	The status of the transaction.

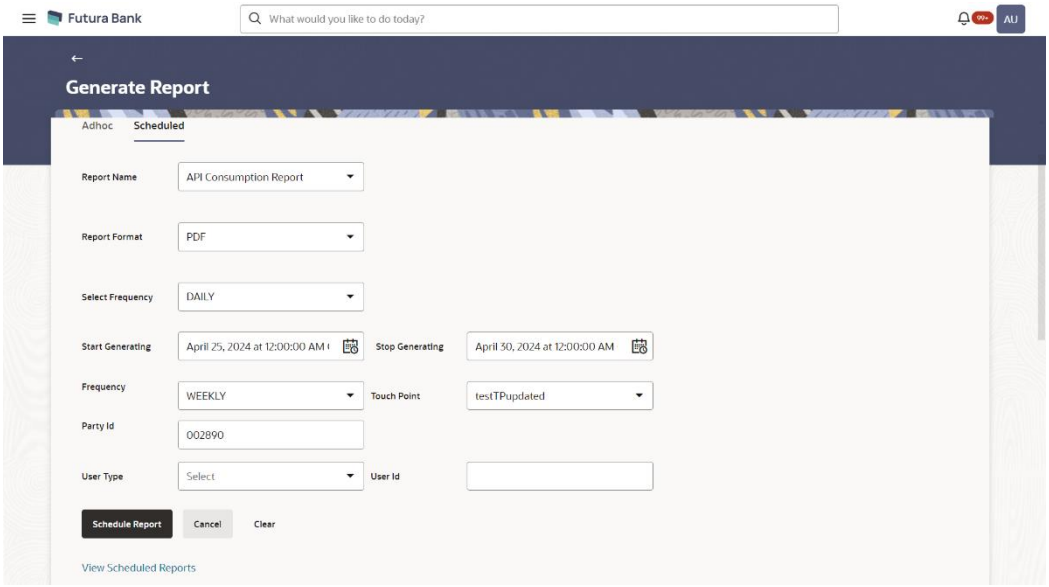
60.3.2 API Consumption - Schedule Reports

The reports that are generated in specific time frame such as daily, weekly, monthly, quarterly, and annually are categorized under scheduled reports.

To generate the API consumption schedule report:

1. Click the **Schedule** tab.
2. From the **Report Name** list, select the appropriate report to be generated. The respective report generation screen appears.

API Consumption Report - Schedule Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV

Field Name	Description
Select Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly
Start Generating	Date from which the report is to be generated as per frequency defined.
Stop Generating	Date till which the report is to be generated as per frequency defined.
Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly
Touch Point	The different channels/ medium for which you want to generate the report.
Party ID	The party ID for whom the report is to be generated.
User Segment	The user segment for which the report is to be generated. The options are: • Corporate User • Retail User • Administrator
User id	The user id of the user for whom report is to be generated.
View Scheduled Reports	Link to view all the reports that are scheduled.

3. From the **Report Format** list, select the appropriate report output format.
4. From the **Select Frequency** list, select the appropriate option.
5. From the **Start Generating** and **Stop Generating** list, select the appropriate duration.
6. From the **Frequency** list, select the appropriate option.
7. From the **Touch Point** list, select the appropriate option.
8. In the **Party ID** field, enter the party id.
9. From the **User Segment** list, select the appropriate segment.

10. In the **User Id** field, enter the id of the user for whom the report is to be generated.
11. Click **Schedule Report** to generate and view the report.
    OR
    Click the **View Scheduled Reports** link to view all the scheduled reports. The **Scheduled Reports** screen appears.
    OR
    Click **Cancel** to cancel the transaction.
    OR
    Click **Clear** to reset the search parameters.
12. The success message along with the reference number, status and **Report Request Id** appears. Click **Ok** to close the screen and navigate to the dashboard.
    OR
    Click on the **View Reports** link to download the report. The user is directed to the My Reports screen. The list of reports appears.
    OR
    Click **Schedule another Report** to generate another report.
13. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports > Scheduled Reports***.

60.4 EPI Payment Reconciliation Report

EPI Payment Reconciliation report provides the status of all reconciled transactions, in a given duration. The user has to select the merchant code for which the report is to be generated,

Further, user has to select a format in which the report needs to be generated. The generation of both Adhoc and Scheduled reports are supported.

How to reach here:

Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

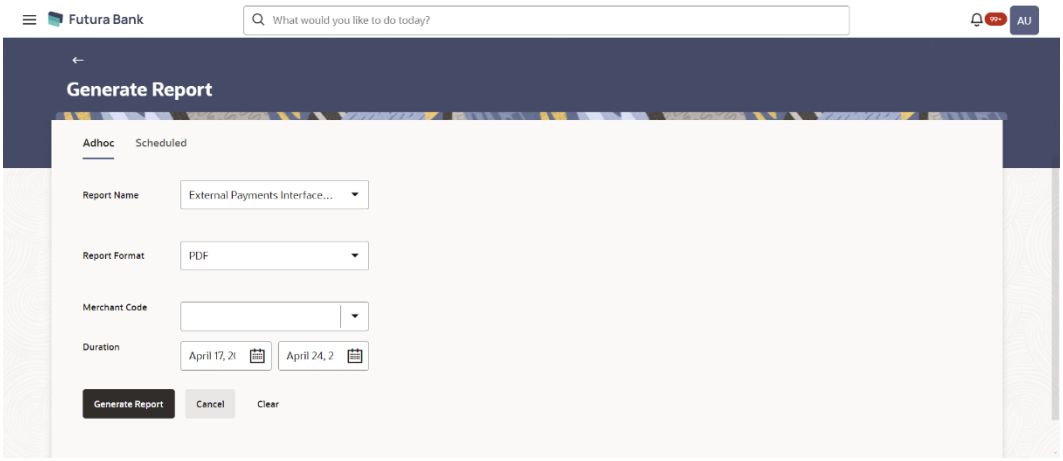
60.4.1 EPI Payment Reconciliation - Adhoc Report

EPI Payment Reconciliation Adhoc reports are generated on demand or on request. Generated reports can be viewed using 'My Reports' screen.

To generate the EPI Payment Reconciliation adhoc report:

1. Click the **Adhoc** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The receptive report generation screen appears.

EPI Payment Reconciliation Report - Adhoc Report



Field Description

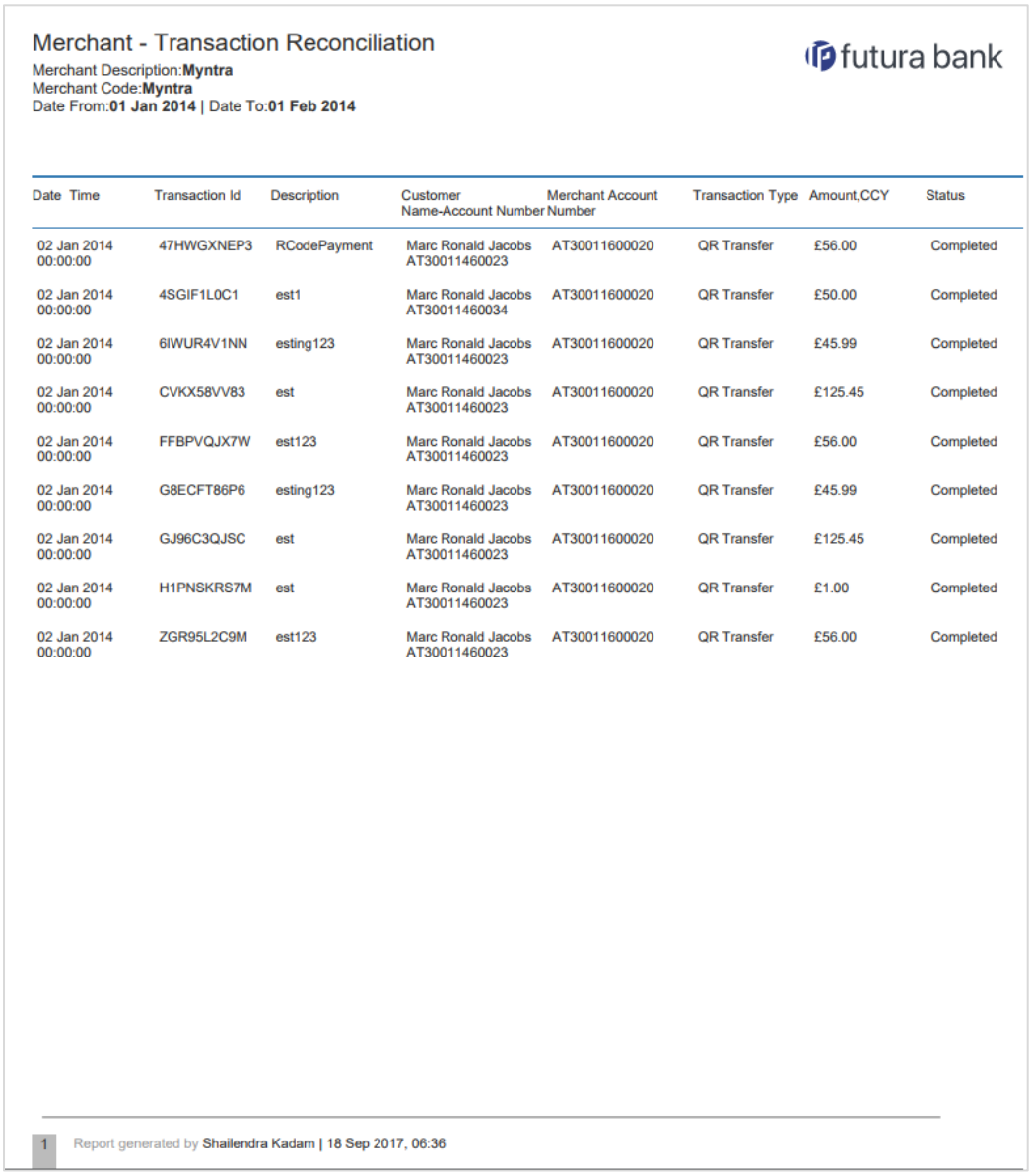
Field Name	Description
Report Name	Select the type of report to be generated.

Field Name	Description
Report Format	Select the format in which the report is to be generated. The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV
Merchant Code	The unique code assigned to a specific merchant by the Bank.
Duration	Specify the date range for which the report is to be generated. User has to enter From and To Date.

3. From the **Report Format** list, select the format in which the report is to be generated.
4. In the **Merchant Code** field, enter the merchant's code for whom the report to be generated.
5. From the **Duration - From** and **Duration - To** list, select the appropriate duration.
6. Click **Generate Report** to generate the report.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
7. The success message along with the reference number, status and **Report Request Id** appears. Click **Ok** to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the **My Reports** screen. The list of reports appears.
   OR
   Click **Generate another report** to generate another report.
8. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. The report will be generated in the format specified at the time of scheduling or generating an adhoc report

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated is given below:



Merchant - Transaction Reconciliation

Merchant Description:**Myntra**
Merchant Code:**Myntra**
Date From:**01 Jan 2014** | Date To:**01 Feb 2014**

futura bank

Date Time	Transaction Id	Description	Customer Name-Account Number	Merchant Account Number	Transaction Type	Amount,CCY	Status
02 Jan 2014 00:00:00	47HWGXNEP3	RCodePayment	Marc Ronald Jacobs AT30011460023	AT30011600020	QR Transfer	£56.00	Completed
02 Jan 2014 00:00:00	4SGIF1L0C1	est1	Marc Ronald Jacobs AT30011460034	AT30011600020	QR Transfer	£50.00	Completed
02 Jan 2014 00:00:00	6IWUR4V1NN	esting123	Marc Ronald Jacobs AT30011460023	AT30011600020	QR Transfer	£45.99	Completed
02 Jan 2014 00:00:00	CVKX58VV83	est	Marc Ronald Jacobs AT30011460023	AT30011600020	QR Transfer	£125.45	Completed
02 Jan 2014 00:00:00	FFBPVQJX7W	est123	Marc Ronald Jacobs AT30011460023	AT30011600020	QR Transfer	£56.00	Completed
02 Jan 2014 00:00:00	G8ECFT86P6	esting123	Marc Ronald Jacobs AT30011460023	AT30011600020	QR Transfer	£45.99	Completed
02 Jan 2014 00:00:00	GJ96C3QJSC	est	Marc Ronald Jacobs AT30011460023	AT30011600020	QR Transfer	£125.45	Completed
02 Jan 2014 00:00:00	H1PNSKRS7M	est	Marc Ronald Jacobs AT30011460023	AT30011600020	QR Transfer	£1.00	Completed
02 Jan 2014 00:00:00	ZGR95L2C9M	est123	Marc Ronald Jacobs AT30011460023	AT30011600020	QR Transfer	£56.00	Completed

1 Report generated by Shailendra Kadam | 18 Sep 2017, 06:36

Field Description

Field Name	Description
Report Parameters	
Merchant Description	The description of the merchant.
Merchant Code	The unique code assigned to a specific merchant by the bank.

Field Name	Description
Date From	The start date of period for which the report is generated.
Date To	The end date of the date for which the report is generated.
Date Time	Transaction date and time.
Transaction ID	The transaction Id of the transaction.
Description	The description of the transaction.
Customer Name-Account Number	The name and account number of the customer.
Merchant Account Number	The merchant's account number.
Transaction Type	The transaction type. The options are: • Sale • Commission
Amount, CCY	The amount of the transaction in local currency.
Status	The status of the transaction.

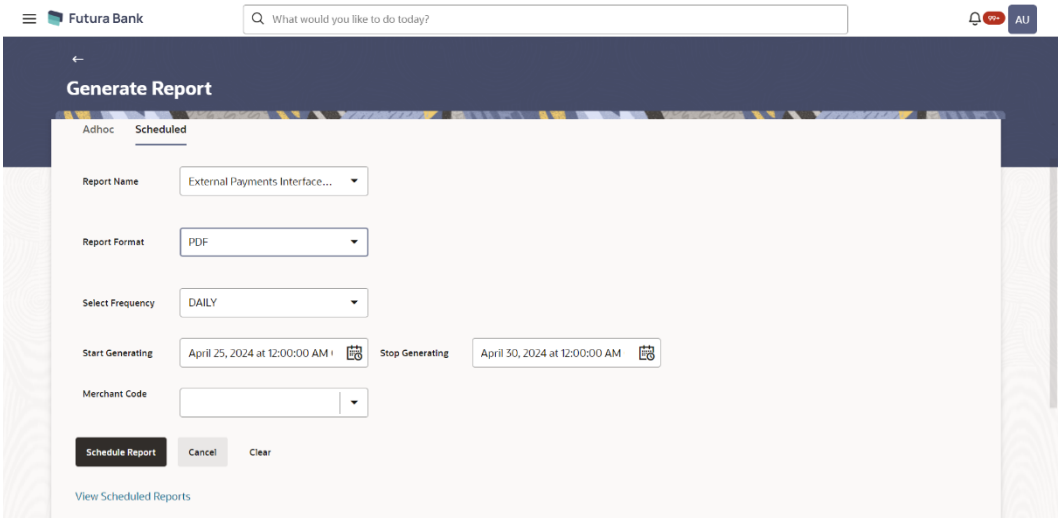
60.4.2 EPI Payment Reconciliation – Schedule Report

The reports that are generated in specific time frame such as daily, weekly, monthly, quarterly, and annually are categorized under scheduled reports.

To generate the EPI Payment Reconciliation scheduled report:

1. Click the **Schedule** tab.
2. From the **Report Name** list, select the appropriate report to be generated. The receptive report generation screen appears.

EPI Payment Reconciliation - Schedule Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated. The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV

Field Name	Description
Select Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly
Start Generating	Date from which the report is to be generated as per the frequency defined.
Stop Generating	Date till which the report is to be generated as per the frequency defined.
Merchant Code	The unique code assigned to a specific merchant by the Bank.
View Scheduled Reports	Link to view all the reports that are scheduled.

3. From the **Report Format** list, select the format in which the report is to be generated.
4. From the **Select Frequency** list, select the appropriate option.
5. From the **Start Generating** and **Stop Generating** list, select the appropriate duration.
6. In the **Merchant Code** field, enter the merchant's code for whom the report to be generated.
7. Click **Schedule Report** to view and generate the report.
   OR
   Click the **View Scheduled Reports** link to view all the scheduled reports. The **Scheduled Reports** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
8. The success message along with the reference number, status and **Report Request Id** appears. Click Ok to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the My Reports screen. The list of reports appears.
   OR
   Click **Schedule another Report** to generate another report.
9. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports > Scheduled Reports***.

60.5 FATCA & CRS Declaration Report

The FATCA & CRS Declaration report contains details related to the information submitted by the users in the forms along with information pertaining to the date and time at which each form was submitted. The administrator can generate separate reports for the FATCA & CRS Self-Certification form for Individuals and the FATCA & CRS Self-Certification form for Entities.

The generation of both Adhoc and Scheduled FATCA & CRS Declaration reports are supported. These reports can be generated in CSV format.

How to reach here:

Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

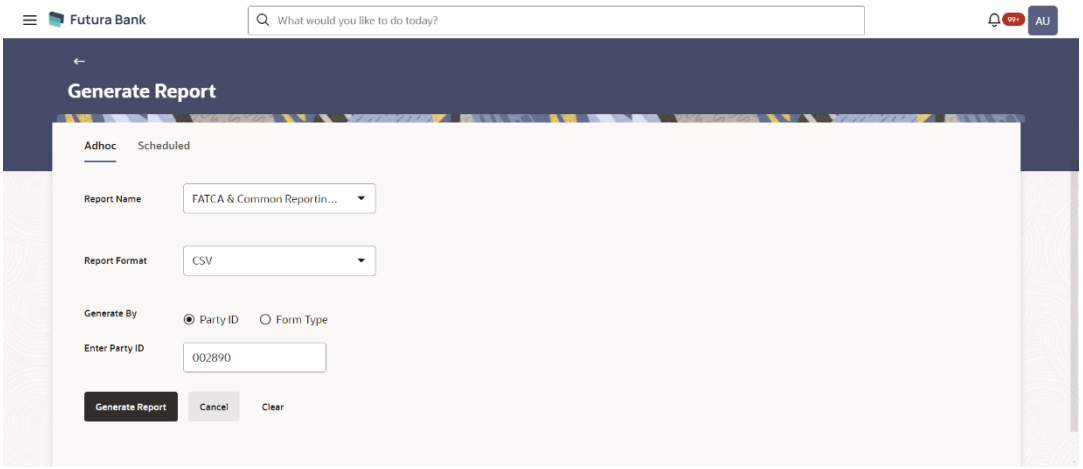
60.5.1 FATCA & CRS Declaration - Adhoc Report

Adhoc reports are generated on demand or on request.

To generate the FATCA & CRS Declaration Adhoc report:

1. Click the **Adhoc** tab.
2. From the **Report Name** list, select the appropriate report to be generated. The respective report generation screen appears.

FATCA & CRS Declaration - Adhoc Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated. The FATCA & CRS Declaration report can be generated in format CSV only.
Generate By	Specify whether the report is to be generated on the basis of party ID or form type as Individual or Entity. The options are: • Party ID • Form Type
Enter Party ID	Specify the party ID of the user for whom report is to be generated. This field appears if you have selected **Party ID** in the **Generate By** field.
Form Type	Select whether you want to generate the report for the FATCA & CRS forms of entities or individuals. The options are: • FATCA & CRS - Entity • FATCA & CRS - Individual This field appears if you have selected **Form Type** in the **Generate By** field.
Duration	Specify the period for which the report is to be generated. • From – The date from which you want to generate the report. • To – The date until which you want to generate the report.

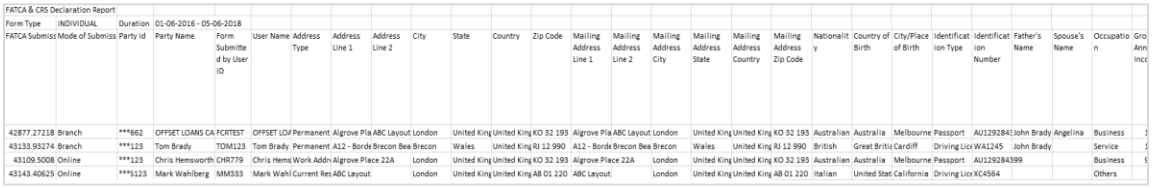
3. From the **Report Format** list, select the format in which the report is to be generated.
4. In the **Generate By** field, select the option of choice.
   a. If you have selected the option **Party ID**, enter the party ID of the user for whom the report is to be generated in the **Enter Party ID** field.
   b. If you have selected the option **Form Type**, select the required form type from the **Form Type** list.
   From the **Duration - From** and **Duration - To** list, select the desired duration.
5. Click **Generate Report** to generate the report.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
6. The success message along with the reference number, status and **Report Request ID** appears. Click **Ok** to close the screen and navigate to the dashboard.
   OR

Click on the **View Reports** link to download the report. The user is directed to the **My Reports** screen. The list of reports appears.
OR
Click **Generate another report** to generate another report.

7. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated for FATCA & CRS form for Individuals is displayed below:



FATCA & CRS Declaration Report																														
Form Type	INDIVIDUAL	Duration	01-06-2016 - 05-06-2018																											
FATCA Submiss	Mode of Submiss	Party Id	Party Name	Form Submitted by User ID	User Name	Address Type	Address Line 1	Address Line 2	City	State	Country	Zip Code	Mailing Address Line 1	Mailing Address Line 2	Mailing Address City	Mailing Address State	Mailing Address Country	Mailing Address Zip Code	Nationality	Country of Birth	City/Place of Birth	Identification Type	Identification Number	Father's Name	Spouse's Name	Occupation	Gro Ann Inco				
42877.27218	Branch	***662	OFFSET LOANS CA	FCRTEST	OFFSET LOA	Permanent	Algrove Pla	ABC Layout	London	United King	United King	KO 32 193	Algrove Pla	ABC Layout	London	United King	United King	KO 32 193	Australian	Australia	Melbourne	Passport	AU129284	John Brady	Angelina	Business					
43133.93274	Branch	***123	Tom Brady	TOM123	Tom Brady	Permanent	A12 - Borde	Brecon Bea	Brecon	Wales	United King	RJ 12 990	A12 - Borde	Brecon Bea	Brecon	Wales	United King	RJ 12 990	British	Great Britai	Cardiff	Driving Lice	WA1245	John Brady		Service					
43109.5008	Online	***123	Chris Hemsworth	CHR779	Chris Hems	Work Addn	Algrove Place	22A	London	United King	United King	KO 32 193	Algrove Place	22A	London	United King	United King	KO 32 193	Australian	Australia	Melbourne	Passport	AU129284399			Business					
43143.40625	Online	***5123	Mark Wahlberg	MM333	Mark Wahl	Current Res	ABC Layout		London	United King	United King	AB 01 220	ABC Layout		London	United King	United King	AB 01 220	Italian	United Stat	California	Driving Lice	XC4564			Others					

Field Description

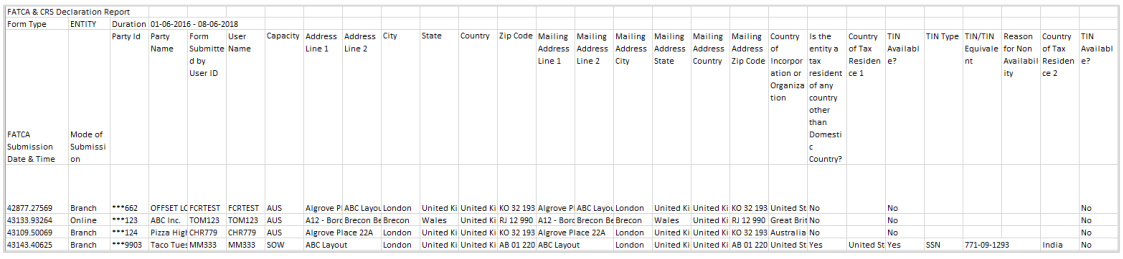
Field Name	Description
FATCA & CRS Declaration report for Individuals	
The following four fields comprise of the criteria on the basis of which the report has been generated.	
Party ID	The party ID of the user who has submitted the form. This field is displayed only if at the time of report generation, the administrator chose to generate the report by specifying a party ID.
Form Type	The type of FATCA & CRS form for which the report is being generated. The form types are: • Entity • Individual
Duration	The period for which the report is generated. This field is displayed only if at the time of report generation, the administrator chose to generate the report on the basis of form type.
The following fields comprise of the main body of the report.	
FATCA Submission Date & Time	The date at time at which the form was submitted by the user.

Field Name	Description
Mode of Submission	The mode through which the form was submitted e.g. online, branch.
Party ID	The party ID of the user who submitted the form.
Party Name	The party name of the user who submitted the form.
Form Submitted by User ID	The user ID of the user who has filled and submitted the FATCA and CRS form.
User Name	The name of the user who has filled and submitted the FATCA and CRS form.
Address Line 1-2	The address details of the user, as entered in the form.
City	The name of the city, as entered in the form.
State	The state, as entered in the form.
Country	The country, as entered in the form.
Zip Code	The zip code of the user, as entered in the form.
Mailing Address Line 1-2	The mailing address of the user, as entered in the form.
Mailing Address City	The city of the user's mailing address, as entered in the form.
Mailing Address State	The state of the user's mailing address, as entered in the form.
Mailing Address Country	The country of the mailing address of the user.
Mailing Address Zip Code	The zip code of the mailing address of the user.
Nationality	The nationality of the user, as entered in the form.
Country of Birth	The country of birth of the user, as entered in the form.
City/ Place of Birth	The city of birth of the user, as entered in the form.
Identification Type	The identification document that serves as proof of identity.
Identification Number	The identification number corresponding to the identification type.

Field Name	Description
Father's Name	The name of the user's father, as entered in the form.
Spouse's Name	The name of the user's spouse, as entered in the form.
Occupation	The employment type of the user, as entered in the form. The occupation type could be any of the following: • Service • Business • Others
Gross Annual Income	The gross annual income that the user enters, as entered in the form.
Politically Exposed Person(PEP) Status	The political status of the user.
Was the Entity established in a country other than <country name>?	The value in this field will identify whether the entity was established in the country in which the bank accounts are held. This field is applicable to sole proprietors only.
Are you a tax resident of any country other than <country name>?	Whether the user is a tax resident of any country other than the country in which the bank accounts are held.
Country of Tax Residence	The name of the country in which the user is a tax resident. A value will be displayed against this field only if the value against the field '**Are you a tax resident of any country other than <country name>?**' is **Yes**.
TIN Available	Whether the user's taxpayer identification number of the country in which he is a tax resident, is available or not. A value will be displayed against this field only if the value against the field '**Are you a tax resident of any country other than <country name>?**' is **Yes**.
Tax Identification Type	The tax identification type of the user. A value will be displayed against this field only if the value against the field '**Are you a tax resident of any country other than <country name>?**' is **Yes** and if the value displayed against '**TIN Available**' is **Yes**.
TIN / TIN Equivalent	The user's taxpayer identification number or equivalent. A value will be displayed against this field only if the value against the field '**Are you a tax resident of any country other than <country name>?**' is **Yes** and if the value displayed against '**TIN Available**' is **Yes**.

Field Name	Description
Reason for Non Availability	The reason for which the user's taxpayer identification number is not available. The user's taxpayer identification number or equivalent. A value will be displayed against this field only if the value against the field '**Are you a tax resident of any country other than <country name>**' is **Yes** and if the value displayed against '**TIN Available**' is **No**.
Are you a citizen of United States of America	Whether the user has a citizenship of the United States of America.
Do you meet the Substantial Presence Test?	Whether the user meets the Substantial Presence Test criteria.
Do you have a green card?	Whether the user holds a United States green card.

For reference, a specimen of the report generated for FATCA & CRS forms for Entities is displayed below:



FATCA & CRS Declaration Report																										
Form Type	ENTITY	Duration	01-06-2016 - 08-06-2018																							
FATCA Submission Date & Time	Mode of Submission	Party Id	Party Name	Form Submitted by User ID	User Name	Capacity	Address Line 1	Address Line 2	City	State	Country	Zip Code	Mailing Address Line 1	Mailing Address Line 2	Mailing Address City	Mailing Address State	Mailing Address Country	Mailing Address Zip Code	Country of Incorporation or Organization	Is the entity a tax resident of any country other than Domestic Country?	Country of Tax Residence 1	TIN Available?	TIN Type	TIN/TIN Equivalent	Reason for Non Availability	Country of Tax Residence 2	TIN Available?
42877.27569	Branch	***662	OFFSET LC	FCRTEST	FCRTEST	AUS	Algrove P	ABC Layou	London	United Ki	United Ki	KO 32 193	Algrove Pl	ABC Layou	London	United Ki	United Ki	KO 32 193	United St	No		No					No
43133.93264	Online	***123	ABC Inc.	TOM123	TOM123	AUS	A12 - Borc	Brecon Be	Brecon	Wales	United Ki	RJ 12 990	A12 - Borc	Brecon Be	Brecon	Wales	United Ki	RJ 12 990	Great Brit	No		No					No
43109.50069	Branch	***124	Pizza High	CHR779	CHR779	AUS	Algrove Place 22A		London	United Ki	United Ki	KO 32 193	Algrove Place 22A		London	United Ki	United Ki	KO 32 193	Australia	No		No					No
43143.40625	Branch	***9903	Taco Tues	MM333	MM333	SOW	ABC Layout		London	United Ki	United Ki	AB 01 220	ABC Layout		London	United Ki	United Ki	AB 01 220	United St	Yes	United St	Yes	SSN	771-09-1293		India	No

Field Description

Field Name	Description
FATCA & CRS Declaration report for Entity	
The following four fields comprise of the criteria on the basis of which the report has been generated.	
Party ID	The party ID of the user who has submitted the form. This field is displayed only if at the time of report generation, the administrator chose to generate the report by specifying a party ID.

Field Name	Description
Form Type	The type of FATCA & CRS form for which the report is being generated. The form types are: • Entity • Individual
Duration	The period for which the report is generated. This field is displayed only if at the time of report generation, the administrator chose to generate the report on the basis of form type.
The following fields comprise of the main body of the report.	
FATCA Submission Date & Time	The date at time at which the form was submitted by the user.
Mode of Submission	The mode through which the form was submitted e.g. online, branch.
Party ID	The party ID of the organization on behalf of which the form was submitted.
Party Name	The party name of the organization on behalf of which the form was submitted.
Form Submitted by User ID	The user id of the user who has filled and submitted the FATCA and CRS form on the behalf of the organization.
User Name	The name of the user who has filled and submitted the FATCA and CRS form on behalf of the organization.
Capacity	The capacity in which the user has submitted the form on behalf of the organization. The values that can be displayed under this column are TRU for trustee, AUS for Authorized Signatory or SOW for Single Ownership.
Address Line 1-2	The address details of the organization.
City	The city name of the organization.
State	The state of the organization.
Country	The country of the organization.
Zip Code	The zip code of the organization.

Field Name	Description
Mailing Address Line 1-2	The mailing address of the organization.
Mailing Address City	The city of the mailing address of the organization.
Mailing Address State	The state of the of the organization's mailing address.
Mailing Address Country	The country of the mailing address of the organization.
Mailing Address Zip Code	The zip code of the mailing address of the organization.
Country of Incorporation or Organization	The country in which the organization was incorporated.
Is the Entity a tax resident of any country other than <country name>?	Whether the entity is a tax resident of country other than country in which the entity's accounts are held within the bank.
Country of Tax Residence	The name of the country in which the organization is a tax resident. A value will be displayed against this field only if the value against the field '**Is the Entity a tax resident of any country other than <country name>?**' is **Yes**.
TIN Available	Whether the organization's taxpayer identification number of the country of which it is a tax resident, is available or not. A value will be displayed against this field only if the value against the field '**Is the Entity a tax resident of any country other than <country name>?**' is **Yes**.
Tax Identification Type	The tax identification type of the organization. A value will be displayed against this field only if the value against the field '**Is the Entity a tax resident of any country other than <country name>?**' is **Yes** and if the value displayed against '**TIN Available**' is **Yes**.
TIN / TIN Equivalent	The taxpayer identification number or equivalent. A value will be displayed against this field only if the value against the field '**Is the Entity a tax resident of any country other than <country name>?**' is **Yes** and if the value displayed against '**TIN Available**' is **Yes**.
Reason for Non Availability	The reason for which the entity's taxpayer identification number is not available. A value will be displayed against this field only if the value against the field '**Is the Entity a tax resident of any country other than <country name>?**' is **Yes** and if the value displayed against '**TIN Available**' is **No**.
Entity incorporated in the United States of America?	Whether the entity was incorporated in the United States of America or not.

Field Name	Description
Entity has any ultimate beneficial owners who are tax residents of countries other than <country name>?	Whether any of the beneficial owners including the controlling persons of the entity/ organization is a tax resident of any country other than the country in which the entity's accounts are held within the bank.
Entity Category	The category to which the entity belongs. The categories are: Financial Institution and Non- Financial Institution.
An Investment Entity located in a Non-Participating Jurisdiction and managed by another Financial Institution	Whether the entity is an investment entity located in a Non-Participating Jurisdiction and managed by another Financial Institution. The value against this field will be Yes or No if the entity is a Financial Institution and an Investment Entity. If the entity is a non-financial institution or a financial institution that is a Depository Institution, Custodial Institution or Specified Insurance Company the value will be NA.
Other Investment Entity	Whether the entity is a type of investment entity that is different from that of an investment entity located in a Non-Participating Jurisdiction and managed by another Financial Institution. The value against this field will be Yes or No if the entity is a Financial Institution and an Investment Entity. If the entity is a non-financial institution or a financial institution that is a Depository Institution, Custodial Institution or Specified Insurance Company the value will be NA.
Depository Institution, Custodial Institution or Specified Insurance Company	Whether the entity is a depository institution, custodial institution or an insurance company. The value against this field will be Yes or No if the entity is a Financial Institution. If the entity is a non-financial institution, the value will be NA.
GIIN Available	Whether the entity's Global Intermediary Identification Number, is available or not. The value against this field will be Yes or No if the entity is a Financial Institution. If the entity is a non-financial institution, the value will be NA.
GIIN	The entity's Global Intermediary Identification Number. The value against this field will be defined if the entity is a Financial Institution and if the value against GIIN Available is Yes. If the entity is a non-financial institution, the value will be NA.
Reason for Non Availability	The reason for which the entity's GIIN is not available. The value against this field will be defined if the entity is a Financial Institution and if the value against GIIN Available is No. If the entity is a non-financial institution, the value will be NA.

Field Name	Description
Active NFE - A corporation, the stock of which is regularly traded on an established securities market	Whether the entity is an active NFE and the entity's stock is regularly traded on an established securities market. The value against this field will be Yes or No if the entity is an Active Non-Financial Institution. If the entity is a financial institution, the value will be NA.
Name of the established securities market on which the corporation is regularly traded	The name of securities market on which the entity trades regularly. The value against this field will be defined if the entity is an Active Non-Financial Institution and is a corporation, the stock of which is regularly traded on an established securities market. The value displayed against this field will be NA if the entity is a financial institution or is any type of non-financial institution other than Active NFE – whose the stock of which is regularly traded on an established securities market.
Active NFE - Entity is related to a corporation whose stock is regularly traded on an established securities market	Whether the entity is an active non-financial entity and is related to a corporation whose stock is regularly traded on an established securities market. The value against this field will be Yes or No if the entity is an Active Non-Financial Institution. If the entity is a financial institution, the value will be NA.
Name of the related corporation whose stock is traded	The name of securities market on which the entity's stock is traded regularly. The value against this field will be defined if the entity is an Active Non-Financial Institution and is related to a corporation whose stock is regularly traded on an established securities market. The value displayed against this field will be NA if the entity is a financial institution or is any type of non-financial institution other than Active NFE and is related to a corporation whose stock is regularly traded on an established securities market.
Nature of relation	The relation that the entity has with the company whose stock is traded. The value against this field will be defined if the entity is an Active Non-Financial Institution and is related to a corporation whose stock is regularly traded on an established securities market. The value displayed against this field will be NA if the entity is a financial institution or is any type of non-financial institution other than Active NFE and is related to a corporation whose stock is regularly traded on an established securities market. The value displayed can be any one of the following: • Subsidiary of the listed company • Controlled by a listed company • Common control as a listed company

Field Name	Description
Name of the established securities market on which the stock of the related corporation is regularly traded	The name of security market in which the stock of the related corporation is traded regularly. The value against this field will be defined if the entity is an Active Non-Financial Institution and is related to a corporation whose stock is regularly traded on an established securities market. The value displayed against this field will be NA if the entity is a financial institution or is any type of non-financial institution other than Active NFE and is related to a corporation whose stock is regularly traded on an established securities market.
Active NFE - A Governmental Entity or Central Bank	Whether the entity is an active non-financial Governmental Entity or Central Bank. The value against this field will be Yes or No if the entity is an Active Non-Financial Institution. If the entity is a financial institution, the value will be NA.
Active NFE - An International Organization	Whether the entity is an active non-financial international organization. The value against this field will be Yes or No if the entity is an Active Non-Financial Institution. If the entity is a financial institution, the value will be NA.
Active NFE - Other - e.g. a start-up NFE or a non-profit NFE	Whether the entity is any other type of active non-financial organization e.g. a start-up NFE or a non-profit NFE. The value against this field will be Yes or No if the entity is an Active Non-Financial Institution. If the entity is a financial institution, the value will be NA.
Sub-Category of Active NFE	The sub-category of the active non- financial entity. The value against this field will be defined if the entity is an Active Non-Financial Institution and is either a government entity or central bank, an international organization or any other type of active NFE. If the entity is a financial institution, the value will be NA.
Passive Non-Financial Entity (NFE)	Specify Whether the entity is a passive non-financial entity. The value against this field will be Yes or No if the entity is a Non-Financial Institution. If the entity is a financial institution, the value will be NA.

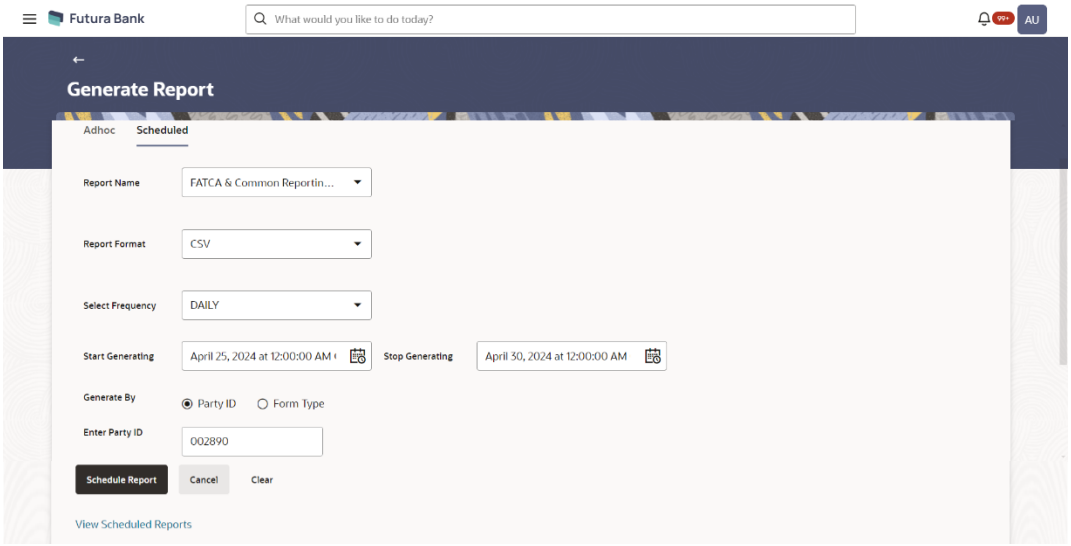
60.5.2 FATCA & CRS Declaration - Schedule Reports

The reports that are generated in a specific time frame such as daily, weekly, monthly, quarterly, and annually are categorized under scheduled reports.

To generate the FATCA & CRS Declaration schedule report:

1. Click the **Schedule** tab.
2. From the **Report Name** list, select **FATCA & CRS Declaration Report** as the report to be generated.
   The respective report generation screen appears.

FATCA & CRS Declaration - Schedule Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated. The FATCA & CRS Declaration report can be generated in format CSV only.
Select Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly

Field Name	Description
Start Generating	Date from which the report is to be generated as per frequency defined.
Stop Generating	Date till which the report is to be generated as per frequency defined.
Generate By	Specify whether the report is to be generated on the basis of party ID or form type as Individual or Entity. The options are: • Party ID • Form Type
Enter Party ID	Specify the party ID of the user for whom report is to be generated. This field appears if you have selected **Party ID** in the **Generate By** field.
Form Type	Select whether you want to generate the report for the FATCA & CRS forms of entities or individuals. The options are: • FATCA & CRS - Entity • FATCA & CRS - Individual This field appears if you have selected **Form Type** in the **Generate By** field.
Duration	Specify the period for which the report is to be generated. • From – The date from which you want to generate the report. • To – The date until which you want to generate the report.
View Scheduled Reports	Link to view all the reports that are scheduled.

3. From the **Report Format** list, select the format in which the report is to be generated.
4. From the **Select Frequency** list, select the appropriate option.
5. From the **Start Generating** and **Stop Generating** list, select the appropriate duration.
6. In the **Generate By** field, select the option of choice.
   a. If you have selected the option **Party ID**, enter the party ID of the user for whom the report is to be generated in the **Enter Party ID** field.
   b. If you have selected the option **Form Type**, select the required form type from the **Form Type** list.

      From the **Duration - From** and **Duration - To** list, select the desired duration.
7. Click **Schedule Report** to view and generate the report.
   OR
   Click the **View Scheduled Reports** link to view all the scheduled reports. The **Scheduled Reports** screen appears.
   OR
   Click **Cancel** to cancel the transaction.

OR
Click **Clear** to reset the search parameters.

8. The success message along with the reference number, status and **Report Request ID** appears. Click **Ok** to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the **My Reports** screen. The list of reports appears.
   OR
   Click **Schedule another Report** to generate another report.
9. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports > Scheduled Reports*.**

60.6 File Identifier wise Party User Mapping Report

File Identifier wise Party User Mapping report provides the summary of user IDs mapped to each file identifiers under a specific party ID. Administrator has to provide a party ID for which the File identifier – user mapping request is to be generated.

Further, user has to select a format in which the report needs to be generated. The generation of both Adhoc and Scheduled reports are supported.

How to reach here:

Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

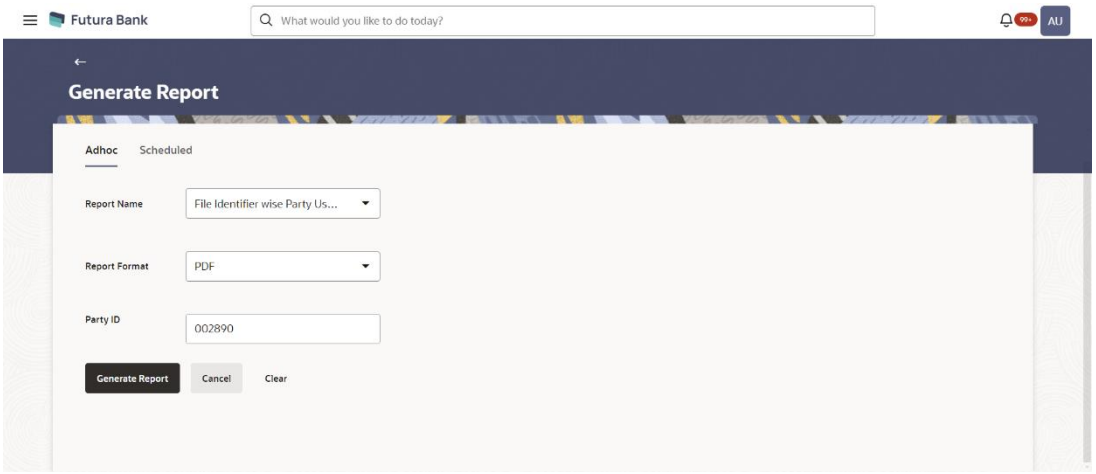
60.6.1 File Identifier wise Party User Mapping - Adhoc Report

File Identifier wise Party User Mapping Adhoc reports are generated on demand or on request. Generated reports can be viewed using 'My Reports' screen.

To generate the File Identifier wise Party User Mapping adhoc report:

1. Click the **Adhoc** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The receptive report generation screen appears.

File Identifier wise Party User Mapping - Adhoc Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated. The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV
Party ID	The ID of party of whom the report is to be generated.

3. From the **Report Format** list, select the format in which the report is to be generated.
4. From the **Frequency** list, select the appropriate option to generate a frequency based report.
5. In the **Party ID** field, enter the party id.
6. Click **Generate Report** to view and generate the report.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
7. The success message along with the reference number, status and **Report Request Id** appears. Click Ok to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the My Reports screen. The list of reports appears.
   OR
   Click **Generate another report** to generate another report.
8. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated is given below:

File Identifier wise Party User Mapping

Party Id: **001164** | Party Name: **Exxon Mobil**

futura bank

File Identifier Code:	MDMCDomABR	Transaction Type : Domestic Funds Transfer	Approval Type: RECORD LEVEL
Sr No	User Name	User Id	
1	Corp Auth1	coprpauth1	
2	Corp Init1	corpinit1	
3	Auto Auth	rkautocorp	
4	Corp User1	rkcorpuser1	
5	Rahul Kamble	rkcorpadmin	

File Identifier Code:	MDMCINTABR	Transaction Type : Internal Funds Transfer	Approval Type: RECORD LEVEL
Sr No	User Name	User Id	
1	Corp Init1	corpinit1	
2	Auto Auth	rkautocorp	
3	Corp User1	rkcorpuser1	

File Identifier Code:	MixePayee	Transaction Type : Mixed Payee	Approval Type: RECORD LEVEL
Sr No	User Name	User Id	
1	Corp User1	rkcorpuser1	

File Identifier Code:	SDMCInternationalABF	Transaction Type : International Funds Transfer	Approval Type: FILE LEVEL
Sr No	User Name	User Id	
1	Corp Init1	corpinit1	
2	Corp User1	rkcorpuser1	
3	Auto Auth	rkautocorp	

File Identifier Code:	SDMCMIXABFile	Transaction Type : Mixed Payments	Approval Type: FILE LEVEL
Sr No	User Name	User Id	
1	Corp User1	rkcorpuser1	

1 Report generated by Suyog Initiator | 12 Oct 2017, 11:29

Field Description

Field Name	Description
Report Parameters	
Party ID	The party ID of whom the report is generated.
Party Name	The name of the party of whom the report is generated.

Field Name	Description
File Identifier Code	The file identifier code mapped to the users.
Transaction Type	The transaction type associated with the file identifier code.
Approval Type	Approval type for the file - either Record or File.
Sr No	Serial number of the records.
User Name	Name of the user to whom the file identifiers are mapped.
User ID	ID of the user.

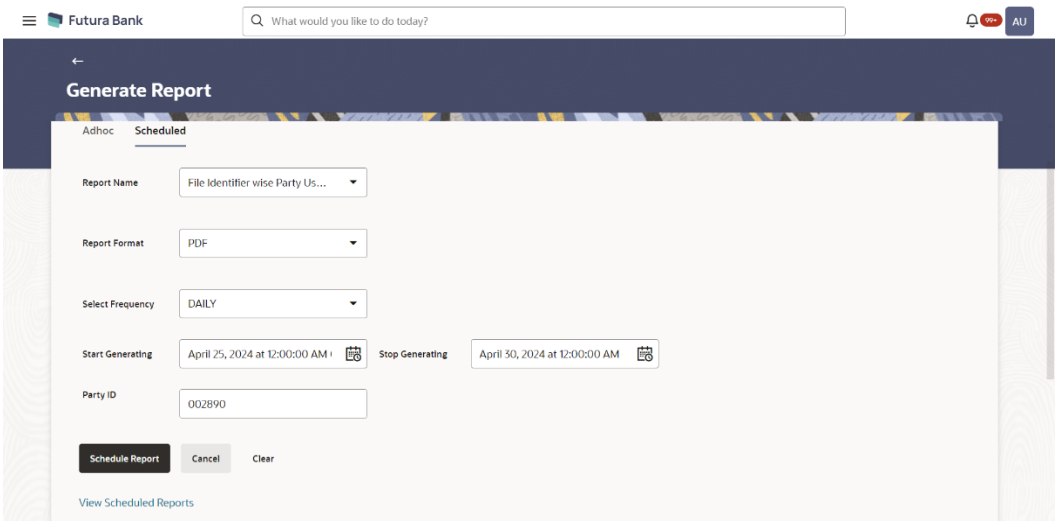
60.6.2 File Identifier wise Party User Mapping - Schedule Report

The reports that are generated in specific time frame such as daily, weekly, monthly, quarterly, and annually are categorized under scheduled reports.

To generate the File Identifier wise Party User Mapping scheduled report:

1. Click the **Schedule** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The receptive report generation screen appears.

File Identifier wise Party User Mapping - Schedule Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV
Select Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly
Start Generating	Date from which the report is to be generated as per the frequency defined
Stop Generating	Date till which the report is to be generated as per the frequency defined.
Party ID	Party ID of whom the report is to be generated.
View Scheduled Reports	Link to view all the reports that are scheduled.

3. From the **Report Format** list, select the format in which the report is to be generated.
4. From the **Select Frequency** list, select the appropriate option.
5. From the **Start Generating** and **Stop Generating** list, select the appropriate duration.
6. In the **Party ID** field, enter the party ID.
7. From the **Duration - From** and **Duration - To** list, select the appropriate duration.
8. Click **Schedule Report** to view and generate the report.
   OR
   Click the **View Scheduled Reports** link to view all the scheduled reports. The **Scheduled Reports** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.

9. The success message along with the reference number, status and **Report Request Id** appears. Click Ok to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the My Reports screen. The list of reports appears.
   OR
   Click **Schedule another Report** to generate another report.
10. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports > Scheduled Reports***.

60.7 Party User wise File Identifiers Mapping Report

Party User wise File Identifiers Mapping Report provides a summary of file identifiers mapped to each user of a specific party. Administrator has to provide a party ID for which the Party User wise File Identifiers Mapping Report is to be generated. Further, user has to select a format in which the report needs to be generated.

The generation of both Adhoc and Scheduled reports are supported.

How to reach here:

Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

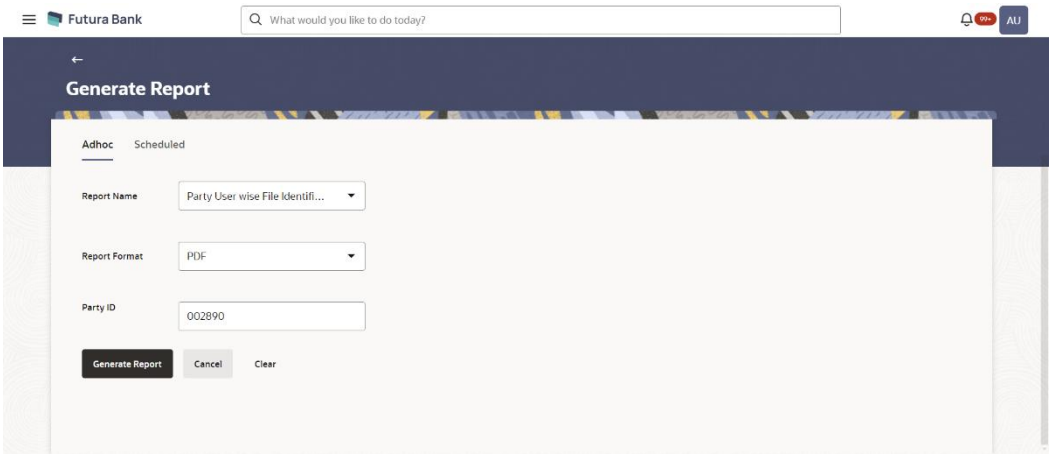
60.7.1 Party User wise File Identifiers Mapping - Adhoc Report

Party User wise File Identifiers Mapping Adhoc reports are generated on demand or on request. Generated reports can be viewed using 'My Reports' screen.

To generate the Party User wise File Identifiers Mapping adhoc report:

1. Click the **Adhoc** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The receptive report generation screen appears.

Party User wise File Identifiers Mapping - Adhoc Reports



Field Description

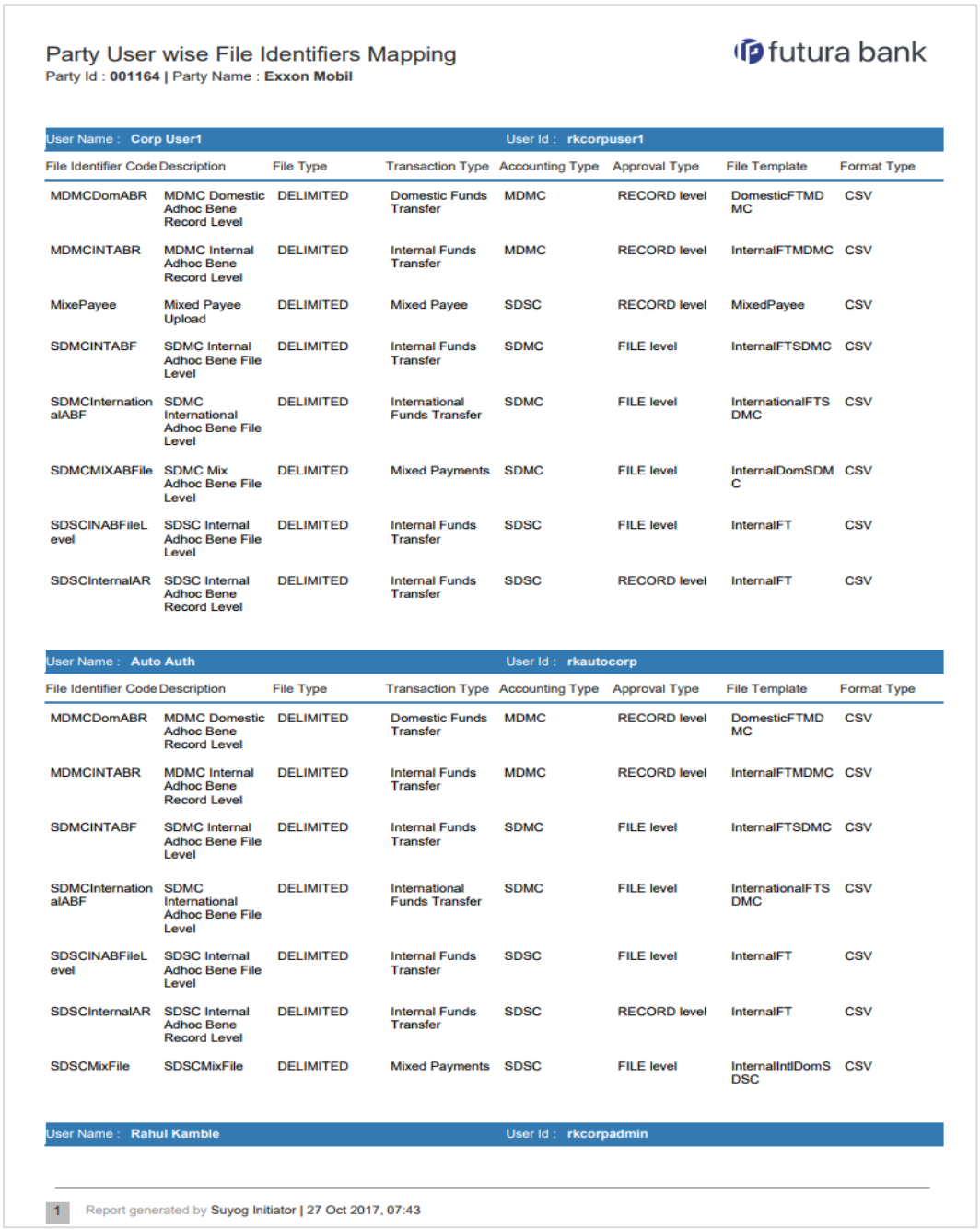
Field Name	Description
Report Name	Select the type of report to be generated.

Field Name	Description
Report Format	Select the format in which the report is to be generated.. The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV
Party ID	Party ID for which the report is to be generated.

3. From the **Report Format** list, select the format in which the report is to be generated.
4. In the **Party ID** field, enter the party id.
5. Click **Generate Report** to view and generate the report.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
6. The success message along with the reference number, status and **Report Request Id** appears. Click Ok to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the **My Reports** screen. The list of reports appears.
   OR
   Click **Generate another report** to generate another report.
7. In the **My reports** screen, click on desired **Report Sub ID** to view and download the generated report.. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated is given below:



Party User wise File Identifiers Mapping

futura bank

Party Id : **001164** | Party Name : **Exxon Mobil**

User Name : **Corp User1** User Id : **rkcorpuser1**

File Identifier Code	Description	File Type	Transaction Type	Accounting Type	Approval Type	File Template	Format Type
MDMCDomABR	MDMC Domestic Adhoc Bene Record Level	DELIMITED	Domestic Funds Transfer	MDMC	RECORD level	DomesticFTMDMC	CSV
MDMCINTABR	MDMC Internal Adhoc Bene Record Level	DELIMITED	Internal Funds Transfer	MDMC	RECORD level	InternalFTMDMC	CSV
MixePayee	Mixed Payee Upload	DELIMITED	Mixed Payee	SDSC	RECORD level	MixedPayee	CSV
SDMCINTABF	SDMC Internal Adhoc Bene File Level	DELIMITED	Internal Funds Transfer	SDMC	FILE level	InternalFTSDMC	CSV
SDMCInternationalABF	SDMC International Adhoc Bene File Level	DELIMITED	International Funds Transfer	SDMC	FILE level	InternationalFTSDMC	CSV
SDMCMIXABFile	SDMC Mix Adhoc Bene File Level	DELIMITED	Mixed Payments	SDMC	FILE level	InternalDomSDMC	CSV
SDSCINABFileLevel	SDSC Internal Adhoc Bene File Level	DELIMITED	Internal Funds Transfer	SDSC	FILE level	InternalFT	CSV
SDSCInternalAR	SDSC Internal Adhoc Bene Record Level	DELIMITED	Internal Funds Transfer	SDSC	RECORD level	InternalFT	CSV

User Name : **Auto Auth** User Id : **rkautocorp**

File Identifier Code	Description	File Type	Transaction Type	Accounting Type	Approval Type	File Template	Format Type
MDMCDomABR	MDMC Domestic Adhoc Bene Record Level	DELIMITED	Domestic Funds Transfer	MDMC	RECORD level	DomesticFTMDMC	CSV
MDMCINTABR	MDMC Internal Adhoc Bene Record Level	DELIMITED	Internal Funds Transfer	MDMC	RECORD level	InternalFTMDMC	CSV
SDMCINTABF	SDMC Internal Adhoc Bene File Level	DELIMITED	Internal Funds Transfer	SDMC	FILE level	InternalFTSDMC	CSV
SDMCInternationalABF	SDMC International Adhoc Bene File Level	DELIMITED	International Funds Transfer	SDMC	FILE level	InternationalFTSDMC	CSV
SDSCINABFileLevel	SDSC Internal Adhoc Bene File Level	DELIMITED	Internal Funds Transfer	SDSC	FILE level	InternalFT	CSV
SDSCInternalAR	SDSC Internal Adhoc Bene Record Level	DELIMITED	Internal Funds Transfer	SDSC	RECORD level	InternalFT	CSV
SDSCMixFile	SDSCMixFile	DELIMITED	Mixed Payments	SDSC	FILE level	InternalIntlDomSDSC	CSV

User Name : **Rahul Kamble** User Id : **rkcorpadmin**

1 Report generated by Suyog Initiator | 27 Oct 2017, 07:43

Field Description

Field Name	Description
Report Parameters	
Party ID	The party ID for which the report is generated.
Party Name	The name of the party for which the report is generated.
User Name	Name of the users to whom the file identifiers are mapped.
User ID	ID of the user
File Identifier Code	The file identifier code mapped to the users.
Description	Description of the file identifier mapped to the user.
File Type	File type of the file identifier mapped to the user.
Transaction Type	Transaction type of the file identifier mapped to the user
Accounting Type	The accounting type of the file identifier mapped to the user.
Approval Type	Approval type of the file identifier mapped to the user
File Template	File template of the file identifier mapped to the user.
Format Type	Format type of the file identifier mapped to the user.

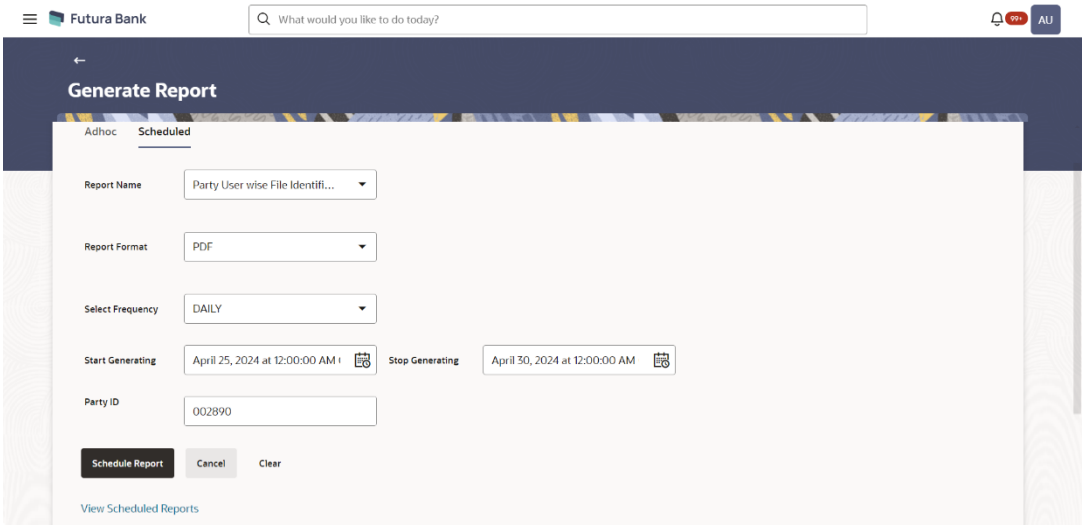
60.7.2 Party User wise File Identifiers Mapping - Schedule Reports

The reports that are generated in specific time frame such as daily, weekly, monthly, quarterly, and annually are categorized under scheduled reports.

To generate the Party User wise File Identifiers Mapping schedule report:

1. Click the **Schedule** tab.
2. From the **Report Name** list, select the appropriate report to be generated. The receptive report generation screen appears.

Party User wise File Identifiers Mapping – Schedule Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated. The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV

Field Name	Description
Select Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly
Start Generating	Date from which the report is to be generated as per the frequency defined.
Stop Generating	Date till which the report is to be generated as per the frequency defined.
Party ID	The party ID for which the report is to be generated.
View Scheduled Reports	Link to view all the reports that are scheduled.

3. From the **Report Format** list, select the format in which the report is to be generated.
4. From the **Select Frequency** list, select the appropriate option.
5. From the **Start Generating** and **Stop Generating list**, select the appropriate duration.
6. In the **Party ID** field, enter the party id.
7. Click **Schedule Report** to view and generate the report.
   OR
   Click the **View Scheduled Reports** link to view all the scheduled reports. The **Scheduled Reports** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
8. The success message along with the reference number, status and **Report Request Id** appears. Click Ok to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the My Reports screen. The list of reports appears.
   OR
   Click **Schedule another Report** to generate another report.
9. In the **My reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports > Scheduled Reports***.

60.8 Party wise File Identifiers Mapping Report

Party wise file identifier mapping report provides summary of file identifiers mapped to a specific party ID. Administrator has to provide a party ID for which Party wise file identifier mapping report is to be generated.

Further, user has to select a format in which the report needs to be generated.

The generation of both Adhoc and Scheduled reports are supported.

How to reach here:

Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

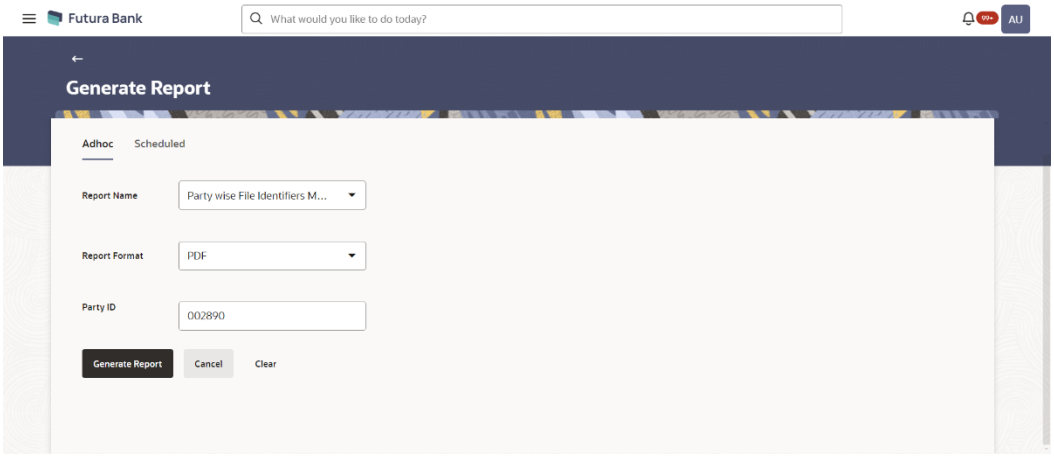
60.8.1 Party wise File Identifiers Mapping - Adhoc Report

Party wise File Identifiers Mapping Adhoc reports are generated on demand or on request. Generated reports can be viewed using 'My Reports' screen.

To generate the Party wise File Identifiers Mapping adhoc report:

1. Click the **Adhoc** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The receptive report generation screen appears.

Party wise File Identifiers Mapping - Adhoc Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.

Field Name	Description
Report Format	Select the format in which the report is to be generated.. The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV
Party ID	Party ID of whom the report is to be generated.

3. From the **Report Format** list, select the format in which the report is to be generated.
4. In the **Party ID** field, enter the party id.
5. Click **Generate Report** to view and generate the report.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
6. The success message along with the reference number, status and **Report Request Id** appears. Click Ok to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the My Reports screen. The list of reports appears.
   OR
   Click **Generate another report** to generate another report.
7. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated is given below:

Party wise File Identifiers Mapping

Party Id : **001164** | Party Name : **Exxon Mobil**

futura bank

Sr No	File Identifier Code	Description	File Type	Transaction Type	Accounting Type	Approval Type	File Template	Format Type
1	MDMCDomABR	MDMC Domestic Adhoc Bene Record Level	DELIMITED	Domestic Funds Transfer	MDMC	RECORD LEVEL	DomesticFTMDMC	CSV
2	MDMCINTABR	MDMC Internal Adhoc Bene Record Level	DELIMITED	Internal Funds Transfer	MDMC	RECORD LEVEL	InternalFTMDMC	CSV
3	MixePayee	Mixed Payee Upload	DELIMITED	Mixed Payee	SDSC	RECORD LEVEL	MixedPayee	CSV
4	SDMCINTABF	SDMC Internal Adhoc Bene File Level	DELIMITED	Internal Funds Transfer	SDMC	FILE LEVEL	InternalFTSDMC	CSV
5	SDMCInternationalABF	SDMC International Adhoc Bene File Level	DELIMITED	International Funds Transfer	SDMC	FILE LEVEL	InternationalFTSDMC	CSV
6	SDMCMIXABFile	SDMC Mix Adhoc Bene File Level	DELIMITED	Mixed Payments	SDMC	FILE LEVEL	InternalDomSDMC	CSV
7	SDSCINABFile Level	SDSC Internal Adhoc Bene File Level	DELIMITED	Internal Funds Transfer	SDSC	FILE LEVEL	InternalFT	CSV
8	SDSCInternalAR	SDSC Internal Adhoc Bene Record Level	DELIMITED	Internal Funds Transfer	SDSC	RECORD LEVEL	InternalFT	CSV
9	SDSCMixFile	SDSCMixFile	DELIMITED	Mixed Payments	SDSC	FILE LEVEL	InternalIntlDomSDSC	CSV

1 Report generated by Mustufa Gari | 27 Oct 2017, 06:37

Field Description

Field Name	Description
Report Parameters	
Party ID	Party ID of whom the report is generated.
Party Name	Party name of whom the report is generated.
Sr No	Serial number of the records.
File Identifier Code	The file identifier codes mapped to the specific party.
Description	Description of file identifiers mapped to the party.
File Type	File type of file identifiers mapped to the party.
Transaction Type	Transaction type of file identifiers mapped to the party.
Accounting Type	The accounting type of file identifiers mapped to the party.
Approval Type	Approval type of file identifiers mapped to the party.
File Template	File template of file identifiers mapped to the party.
Format Type	Format type of file identifiers mapped to the party..

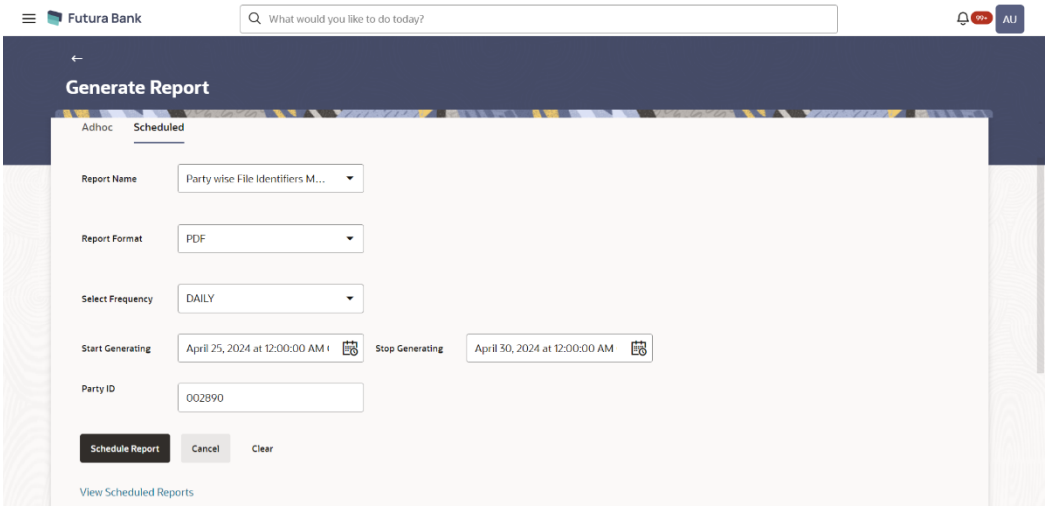
60.8.2 Party wise File Identifiers Mapping - Schedule Reports

The reports that are generated in specific time frame such as daily, weekly, monthly, quarterly, and annually are categorized under scheduled reports.

To generate the Party wise File Identifiers Mapping schedule report:

1. Click the **Schedule** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The receptive report generation screen appears.

Party wise File Identifiers Mapping - Schedule Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated.. The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV

Field Name	Description
Select Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly
Start Generating	Date from which the report is to be generated as per the frequency defined.
Stop Generating	Date till which the report is to be generated as per the frequency defined,
Party ID	Party ID of which the report is to be generated.
View Scheduled Reports	Link to view all the reports that are scheduled.

3. From the **Report Format** list, select the format in which the report is to be generated.
4. From the **Select Frequency** list, select the appropriate option.
5. From the **Start Generating** and **Stop Generating list**, select the appropriate duration.
6. In the **Party ID** field, enter the party id.
7. Click **Schedule Report** to view and generate the report.
   OR
   Click the **View Scheduled Reports** link to view all the scheduled reports. The **Scheduled Reports** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
8. The success message along with the reference number, status and **Report Request Id** appears. Click Ok to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the My Reports screen. The list of reports appears.
   OR
   Click **Schedule another Report** to generate another report.
9. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports > Scheduled Reports***.

60.9 Approval Rule Report

Approval Rule Report provides the list of rules and workflows belonging to a group corporate. Administrator has to provide a party ID for which the Approval Rule Report is to be generated.

System Administrator has to select a format in which the report needs to be generated. This report can be generated only on an Adhoc basis and is not available under ‘Schedule’ option.

How to reach here:

Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

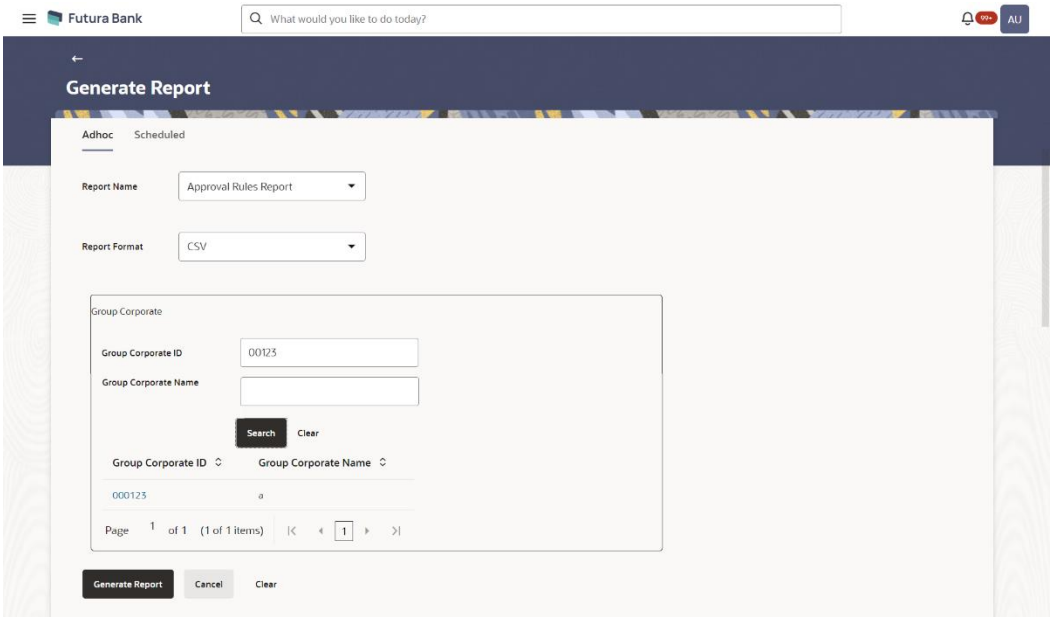
60.9.1 Approval Rule Report - Adhoc Report

Approval Rule Adhoc reports are generated on demand or on request. Generated reports can be viewed using ‘My Reports’ screen.

To generate the Approval Rule adhoc report:

1. Click the **Adhoc** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The receptive report generation screen appears.

Approval Rule Report - Adhoc Reports



Field Description

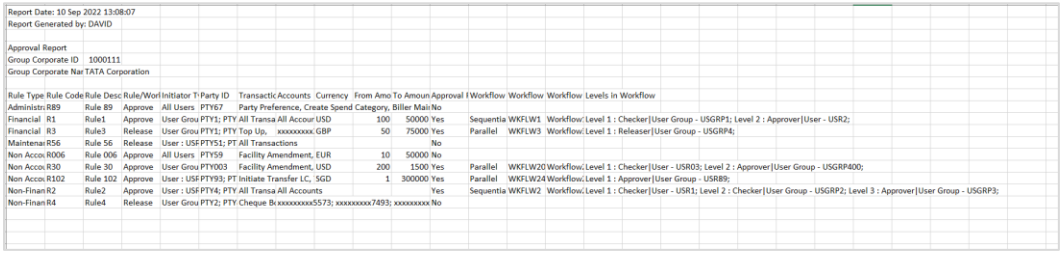
Field Name	Description
Report Name	Select the type of report to be generated.

Field Name	Description
Report Format	Select the format in which the report is to be generated. The approval rule report can be generated in format CSV only.
Group Corporate ID	The Group Corporate ID of the user for whom report has been generated
Group Corporate Name	The Group Corporate Name of the user for whom report has been generated

3. From the **Report Format** list, select the format in which the report is to be generated.
4. In the **Group Corporate ID** field, enter the Group Corporate ID.
5. In the **Group Corporate Name** field, enter the Group Corporate name.
6. Click **Generate Report** to view and generate the report.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
7. The success message along with the reference number, status and **Report Request Id** appears. Click **Ok** to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the **My Reports** screen. The list of reports appears.
   OR
   Click **Generate another report** to generate another report.
8. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated is given below:



Report Date: 10 Sep 2022 13:08:07
Report Generated by: DAVID

Approval Report
Group Corporate ID 1000111
Group Corporate Nar TATA Corporation

Rule Type	Rule Code	Rule Desc	Rule/Worl	Initiator T	Party ID	Transactic	Accounts	Currency	From Amo	To Amoun	Approval I	Workflow	Workflow	Workflow	Levels In Workflow
Administr	R89	Rule 89	Approve	All Users	PTY67	Party Preference, Create Spend Category, Biller Mai					No				
Financial	R1	Rule1	Approve	User Grou	PTY1; PTY	All Transa	All Accour	USD	100	50000	Yes	Sequentia	WKFLW1	Workflow	Level 1 : Checker|User Group - USGRP1; Level 2 : Approver|User - USR2;
Financial	R3	Rule3	Release	User Grou	PTY1; PTY	Top Up,	xxxxxxxxx	GBP	50	75000	Yes	Parallel	WKFLW3	Workflow	Level 1 : Releaser|User Group - USGRP4;
Maintenar	R56	Rule 56	Release	User : USF	PTY51; PT	All Transactions					No				
Non Accou	R006	Rule 006	Approve	All Users	PTY59	Facility Amendment,		EUR	10	50000	No				
Non Accou	R30	Rule 30	Approve	User Grou	PTY003	Facility Amendment,		USD	200	1500	Yes	Parallel	WKFLW20	Workflow	Level 1 : Checker|User - USR03; Level 2 : Approver|User Group - USGRP400;
Non Accou	R102	Rule 102	Approve	User : USF	PTY93; PT	Initiate Transfer LC,		SGD	1	300000	Yes	Parallel	WKFLW24	Workflow	Level 1 : Approver|User Group - USR89;
Non-Finan	R2	Rule2	Approve	User : USF	PTY4; PTY	All Transa	All Accounts				Yes	Sequentia	WKFLW2	Workflow	Level 1 : Checker|User - USR1; Level 2 : Checker|User Group - USGRP2; Level 3 : Approver|User Group - USGRP3;
Non-Finan	R4	Rule4	Release	User Grou	PTY2; PTY	Cheque Bo	xxxxxxxxx	5573; xxxxxxxxx	7493; xxxxxxxxx		No				

Field Description

Field Name	Description
Report Parameters	
Group Corporate ID	The Group Corporate ID of the user for whom report has been generated
Group Corporate Name	The Group Corporate Name of the user for whom report has been generated
Rule Type	Transaction rule type for which the approval rule is set up.
Rule Code	Approval rule code.
Rule Description	Approval rule description.
Rule/Workflow Applicable For	User name /group name of the user maintained in a workflow at level.
Initiator Type	Initiator type specified while creating a rule.
Party ID	Party ID of workflow.
Transactions	Transaction for which the rule is set up.
Accounts	Accounts for which the rule is set up.
Currency	Currency set for the rule.
From Amount	The minimum amount for the transactions allowed for the user.
To Amount	The maximum amount for the transactions allowed for the user.
Approval Required	Field displays whether approval is required or not for the set condition.

Field Name	Description
Workflow Preference	The preference of the approval workflow.
Workflow Code	Code of the approval workflow.
Workflow Description	The approval workflow description.
Levels in Workflow	Approval levels for a user / user group.

60.10 User Segment Summary Report

User Segment Summary Report enables the System Administrator user to view the count of users mapped to a segment.

System Administrator has to select a format in which the report needs to be generated. Generation of both Adhoc and Scheduled reports are supported.

How to reach here:

Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

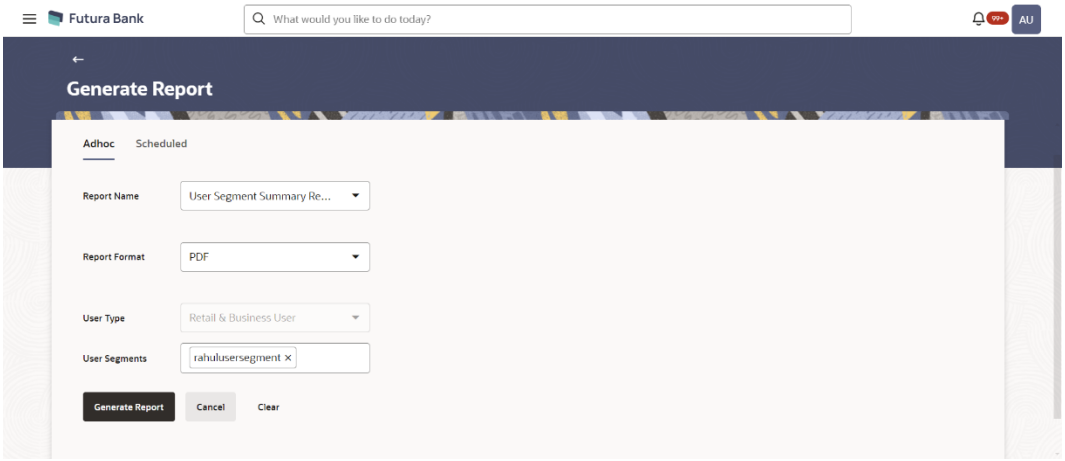
60.10.1 User Segment Summary - Adhoc Report

User Segment Summary Report Adhoc reports are generated on demand or on request. Reports can be requested from the 'Reports' screen. Adhoc reports can be viewed using 'My Reports' screen.

To generate the User Segment Summary adhoc report:

1. Click the **Adhoc** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The respective report generation screen appears.

User Segment Summary Report - Adhoc Report



Field Description

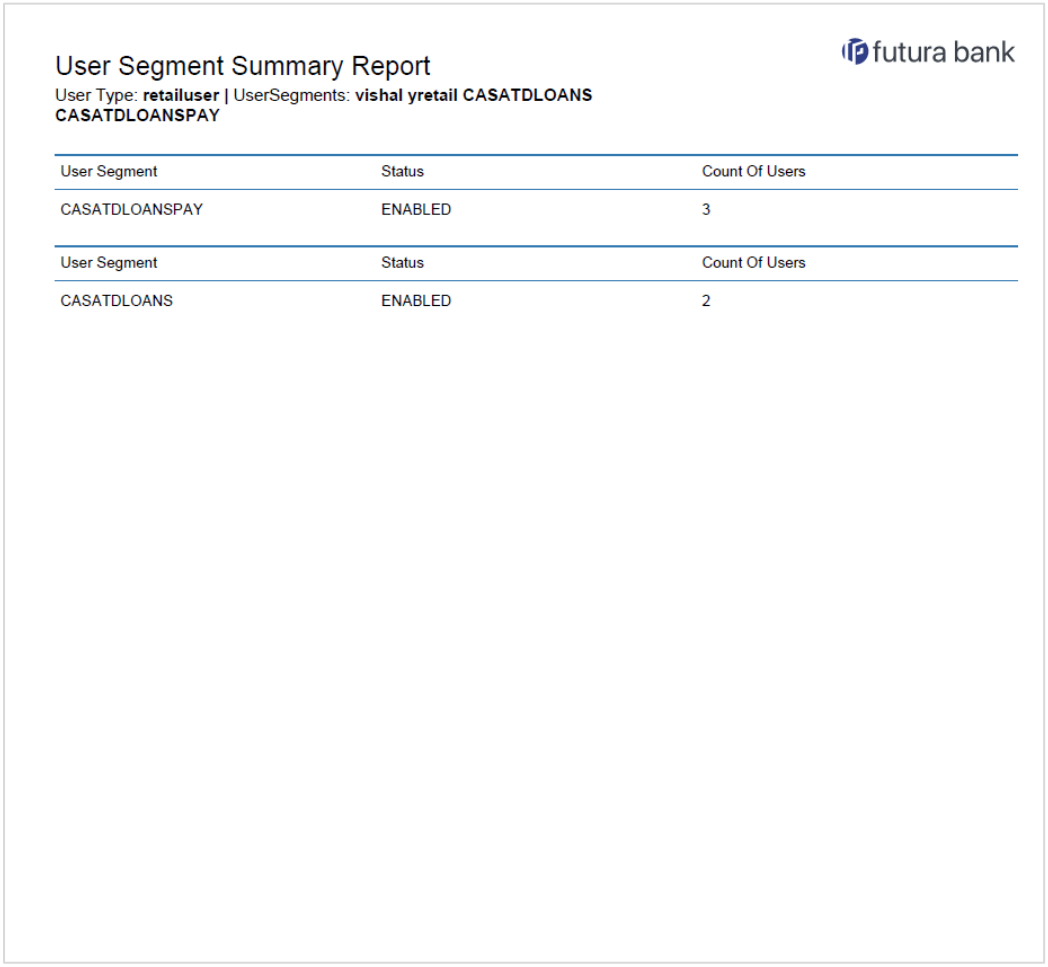
Field Name	Description
Report Name	Select the type of report to be generated.

Field Name	Description
Report Format	Select the format in which the report is to be generated The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV
User Type	The user type for which, the report is generated. The options are: • Corporate User • Administrator User • Retail User
User Segment	The user segment for which the report is to be generated.

3. From the **Report Format** list, select the appropriate report output format.
4. From the **User Type** list, select the appropriate type of user.
5. From the **User Segment** list, select the appropriate user segment.
6. Click **Generate Report** to generate the report.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
7. The success message along with the reference number, status and **Report Request Id** appears. Click **Ok** to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the **My Reports** screen. The list of reports appears.
   OR
   Click **Generate another report** to generate another report.
8. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated is given below:



futura bank

User Segment Summary Report

User Type: **retailuser** | UserSegments: **vishal yretail CASATDLOANS CASATDLOANSPAY**

User Segment	Status	Count Of Users
CASATDLOANSPAY	ENABLED	3

User Segment	Status	Count Of Users
CASATDLOANS	ENABLED	2

Field Description

Field Name	Description
Report Parameters	
User Type	The user type for which, the report is generated.
User Segments	The user segments mapped to the user type.
User Segment	The user segment for which, the report is generated.
Status	The status of the transaction.
Count of Users	The count of users mapped to a segment for which, the report is generated.

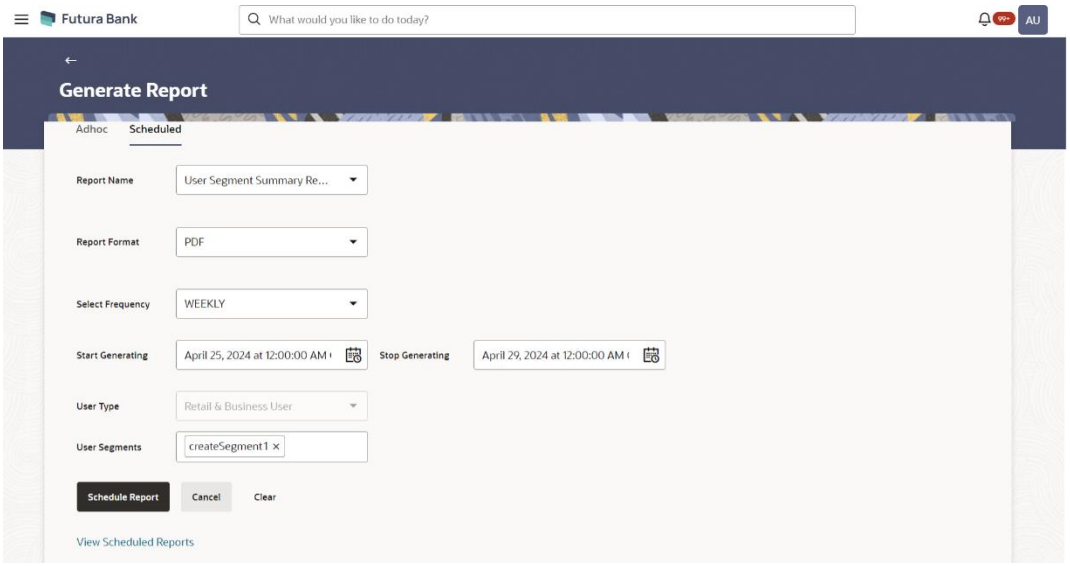
60.10.2 User Segment Summary - Schedule Reports

The reports that are generated in specific time frame such as daily, weekly, monthly, quarterly, and annually are categorized under scheduled reports.

To generate the user segment summary schedule report:

1. Click the **Schedule** tab.
2. From the **Report Name** list, select the appropriate report to be generated.
   The respective report generation screen appears.

User Segment Summary - Schedule Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV

Field Name	Description
Select Frequency	Select the frequency at which the report is to be generated. The options are: • Once • Daily • Weekly • Monthly
Start Generating	Date from which the report is to be generated as per frequency defined.
Stop Generating	Date till which the report is to be generated as per frequency defined.
User Type	The user type for which, the report is generated. The options are: • Corporate User • Administrator User • Retail User
User Segment	The user segment for which the report is to be generated.
View Scheduled Reports	Link to view all the reports that are scheduled.

3. From the **Report Format** list, select the appropriate report output format.
4. From the **Select Frequency** list, select the appropriate option.
5. From the **Start Generating** and **Stop Generating** list, select the appropriate duration.
6. From the **User Type** list, select the appropriate type of user.
7. From the **User Segments** list, select the appropriate user segment.
8. Click **Schedule Report** to generate and view the report.
   OR
   Click the **View Scheduled Reports** link to view all the scheduled reports. The **Scheduled Reports** screen appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
9. The success message along with the reference number, status and **Report Request Id** appears. Click **Ok** to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the My Reports screen. The list of reports appears.
   OR
   Click **Schedule another Report** to generate another report.

10. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports > Scheduled Reports***.

60.11 User Entitlement Report

User Entitlement Report enables the System Administrator user to view the details of corporate user's entitlement within the OBDX application.

System Administrator has to select a format in which the report needs to be generated. The User Entitlement Report supports only Adhoc report generation. This report will not be available under 'Schedule' option.

How to reach here:

Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

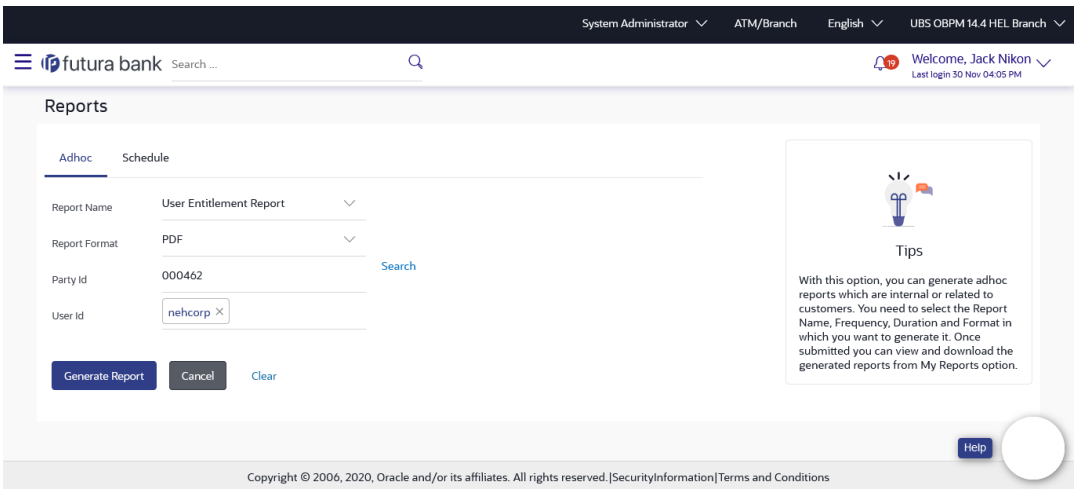
60.11.1 User Entitlement Report- Adhoc Report

User Entitlement Adhoc reports are generated on demand or on request. Reports can be requested from the 'Reports' screen. Adhoc reports can be viewed using 'My Reports' screen.

To generate the User Entitlement adhoc Report:

1. Click the **Adhoc** tab.
2. From the **Report Name** list, select the appropriate report to be generated. The respective report generation screen appears.

User Entitlement Report - Adhoc Report



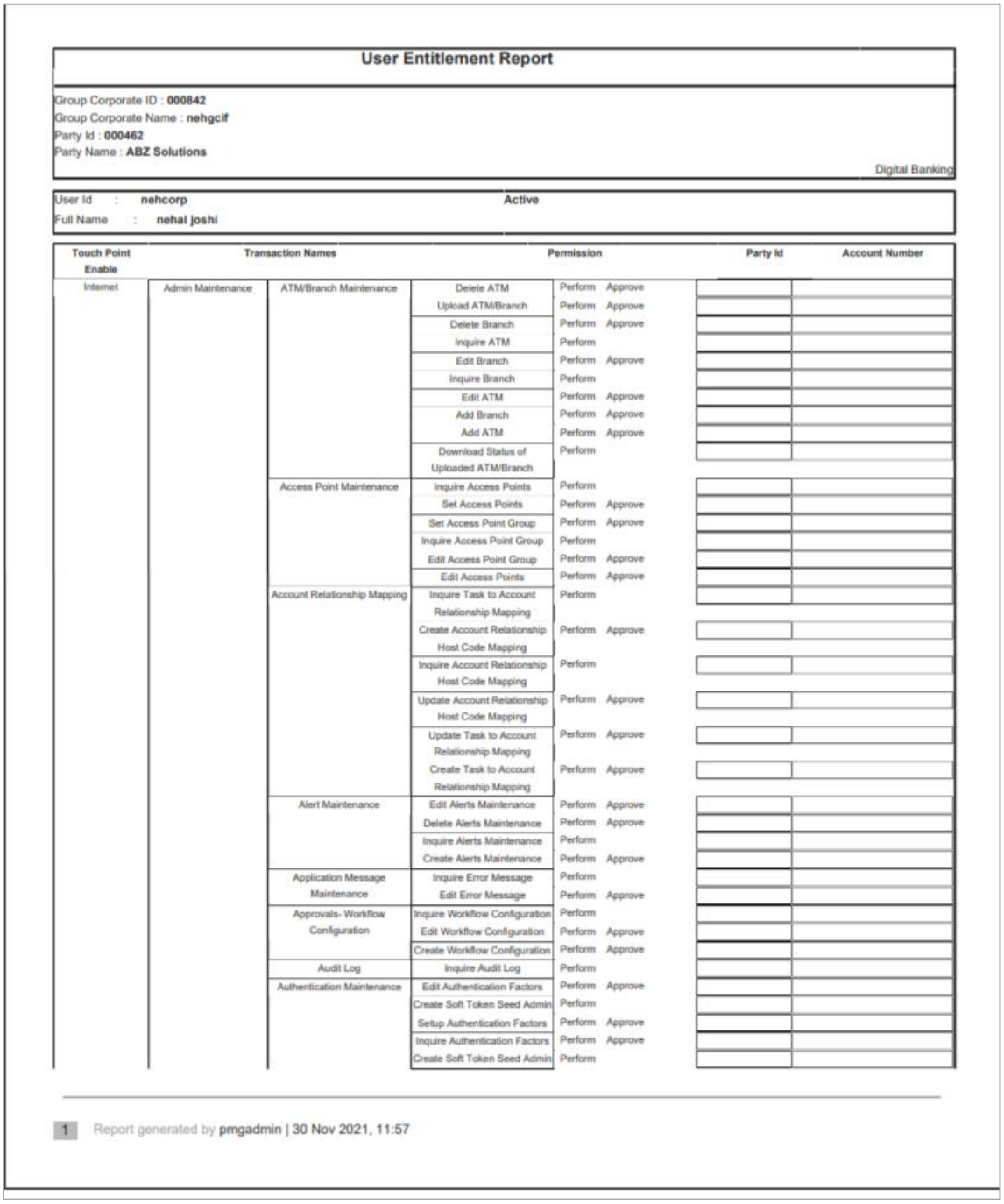
Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated The options with Oracle Analytics Publisher are: • PDF • XLS The options with Internal Reporting Application are: • PDF • CSV
Party ID	The party ID of the user for whom the report is to be generated.
User id	The user id of the user for whom the report is to be generated.

3. From the **Report Format** list, select the appropriate report output format.
4. In the **Party ID** field, enter the party id & click on '**Search'**
5. From the **User Id** list, select the appropriate id of the user for whom the report is to be generated.
6. Click **Generate Report** to generate the report.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Clear** to reset the search parameters.
7. The success message along with the reference number, status and **Report Request Id** appears. Click **Ok** to close the screen and navigate to the dashboard.
   OR
   Click on the **View Reports** link to download the report. The user is directed to the **My Reports** screen. The list of reports appears.
   OR
   Click **Generate another report** to generate another report.
8. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated is given below:



User Entitlement Report

Group Corporate ID : **000842**
Group Corporate Name : **nehgcif**
Party Id : **000462**
Party Name : **ABZ Solutions**

Digital Banking

User Id : **nehcorp** **Active**
Full Name : **nehal joshi**

Touch Point Enable	Transaction Names		Permission			Party Id	Account Number
Internet	Admin Maintenance	ATM/Branch Maintenance	Delete ATM	Perform	Approve		
			Upload ATM/Branch	Perform	Approve		
			Delete Branch	Perform	Approve		
			Inquire ATM	Perform			
			Edit Branch	Perform	Approve		
			Inquire Branch	Perform			
			Edit ATM	Perform	Approve		
			Add Branch	Perform	Approve		
			Add ATM	Perform	Approve		
			Download Status of Uploaded ATM/Branch	Perform			
		Access Point Maintenance	Inquire Access Points	Perform			
			Set Access Points	Perform	Approve		
			Set Access Point Group	Perform	Approve		
			Inquire Access Point Group	Perform			
			Edit Access Point Group	Perform	Approve		
			Edit Access Points	Perform	Approve		
		Account Relationship Mapping	Inquire Task to Account Relationship Mapping	Perform			
			Create Account Relationship Host Code Mapping	Perform	Approve		
			Inquire Account Relationship Host Code Mapping	Perform			
			Update Account Relationship Host Code Mapping	Perform	Approve		
			Update Task to Account Relationship Mapping	Perform	Approve		
			Create Task to Account Relationship Mapping	Perform	Approve		
		Alert Maintenance	Edit Alerts Maintenance	Perform	Approve		
			Delete Alerts Maintenance	Perform	Approve		
			Inquire Alerts Maintenance	Perform			
			Create Alerts Maintenance	Perform	Approve		
		Application Message Maintenance	Inquire Error Message	Perform			
			Edit Error Message	Perform	Approve		
		Approvals- Workflow Configuration	Inquire Workflow Configuration	Perform			
			Edit Workflow Configuration	Perform	Approve		
			Create Workflow Configuration	Perform	Approve		
		Audit Log	Inquire Audit Log	Perform			
		Authentication Maintenance	Edit Authentication Factors	Perform	Approve		
			Create Soft Token Seed Admin	Perform			
			Setup Authentication Factors	Perform	Approve		
			Inquire Authentication Factors	Perform	Approve		
			Create Soft Token Seed Admin	Perform			

1 Report generated by pmgadmin | 30 Nov 2021, 11:57

Field Description

Field Name	Description
Report Parameters	

Field Name	Description
Group Corporate ID	The Group Corporate ID of the user for whom report has been generated
Group Corporate Name	The Group Corporate Name of the user for whom report has been generated
Party ID	The party ID of the user for whom the report has been generated.
Party Name	The party Name of the user for whom the report has been generated.
User ID	The user id of the user for whom the report has been generated.
User Status	The User Status in the OBDX application
Report Details	
Touch Point Enable	The touch points enabled for the User to access the application
Transaction Name	The accessible transaction for the user
Permission	The permission to access the transaction whether its perform, Approve or view
Party ID	The Party ID of Accessible Transactions Account number
Account Number	The Account number to which user has access to perform the transactions.

60.12 User List Report

User List Report enables the System Administrator user to view the list of users belonging to a specific party/group corporate ID.

System Administrator has to select a format in which the report needs to be generated. The User List Report supports only Adhoc report generation. This report will not be available under ‘Schedule’ option.

How to reach here:

System/Bank Administrator Dashboard > Toggle menu > Menu > Reports > Report Generation

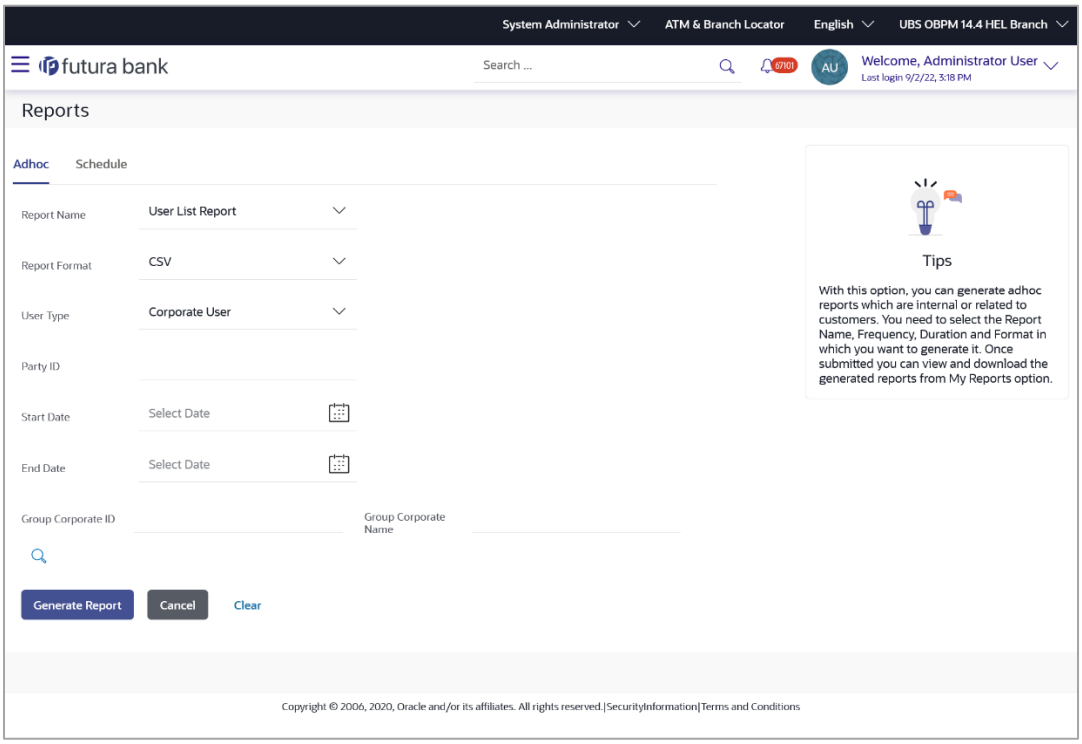
60.12.1 User List Report- Adhoc Report

User Adhoc reports are generated on demand or on request. Reports can be requested from the 'Reports' screen. Adhoc reports can be viewed using 'My Reports' screen.

To generate the User List adhoc Report:

9. Click the **Adhoc** tab.
10. From the **Report Name** list, select the appropriate report to be generated. The respective report generation screen appears.

User List Report - Adhoc Report



Field Description

Field Name	Description
Report Name	Select the type of report to be generated.
Report Format	Select the format in which the report is to be generated The options with Oracle Analytics Publisher are: • CSV
User Type	The user type for whom the report is to be generated.
Party ID	The party ID of the user for whom the report is to be generated.
Duration	The period for which the report is to be generated. Start date of the date range from which you want to generate the report. End date of the date range up-to which you want to generate the report
Group Corporate ID	The group corporate ID for whom the report is to be generated. Note: This field is displayed only for a Corporate user. For a corporate user, if both Group Corporate ID and Party ID is provided, then all users belonging to the given Group Corporate and having given party as the 'Primary Party' of the 'Primary Entity' will be listed in the report .
Group Corporate Name	The group corporate name for whom the report is to be generated.

11. From the **Report Format** list, select the appropriate report output format.
12. From the **User Type** list, select the desired user for whom report to be generated.
13. In the **Party ID** field, enter the party ID.
14. From the **Duration - From Date** and **Duration - To Date** list, select the appropriate duration.
15. In the **Group Corporate ID** field, enter the appropriate id of the Group Corporate ID for whom the report is to be generated.
    OR
    In the **Group Corporate Name** field, enter the name of the Group Corporate for whom the report is to be generated.
16. Click on icon. Based on entered details, the Group Corporate ID and Name appears,
17. Select appropriate Group Corporate ID for whom report is to be generated.
    OR
    Click **Clear** to reset the search parameters.
18. Click **Generate Report** to view & generate the report.
    OR
    Click **Cancel** to cancel the transaction.

OR
Click **Clear** to reset the search parameters.

19. The success message along with the reference number, status and **Report Request Id** appears. Click **Ok** to close the screen and navigate to the dashboard.
    OR
    Click on the **View Reports** link to download the report. The user is directed to the **My Reports** screen. The list of reports appears.
    OR
    Click **Generate another Adhoc Report** to generate another report.
20. In the **My Reports** screen, click on desired **Report Sub ID** to view and download the generated report. A report will be generated in the format specified at the time of scheduling or generating an adhoc report.

Note: You can also download the requested report from ***Administrator Dashboard > Toggle Menu > Reports > My Reports***.

For reference, a specimen of the report generated is given below:

User List Report-Corporate.csv

Field Description

Field Name	Description
Report Parameters	
User Type	The Type of the user for whom the report has been generated.
Party ID	The party ID of the user for whom the report has been generated.
Group Corporate ID	The Group Corporate ID of the user for whom report has been generated
Start Date	Date from which the report is generated.
End Date	Date till which the report is generated.
Group Corporate ID	The Group Corporate ID of the user for whom report has been generated
Group Corporate Name	The group corporate name of the user for whom report has been generated
User Name	The user name of the user for whom the report has been generated.
Title	Title of the user.

Field Name	Description
First Name	First name of the user.
Middle Name	Middle name of the user.
Last Name	Last name of the user.
Date of Birth	Date of birth of the user.
Email ID	Email ID of the user.
Contact Number	Contact number of the user.
Status	Status of the user.
Touchpoints	Name of the touch points.
Primary Entity	Name of the primary entity.
Primary Party	Name of the primary party.
Accessible Party	Name of the accessible party.
Accessible Entity	Name of the accessible entity.
Primary Party (Accessible Entity)	Name of the primary entity.
Accessible Party (Accessible Entity)	Name of the accessible party.
Roles	Details of user role.
User Creation Date/Time	Details of user creation date/time.
Created By	Name of the user who created report.

61. My Reports

This option enables the user to download the adhoc/scheduled reports generated using Report Generation screen. On accessing ‘My Reports’ menu, last 10 reports which generated by the system are listed with the respective report status. User can choose to search the specific report using the search criteria or can opt to view/ download detailed report.

The reports generated on adhoc basis will appear under ‘Adhoc’ tab, whereas the scheduled reports generated as per set frequency will appear under ‘Scheduled’ tab.

How to reach here:

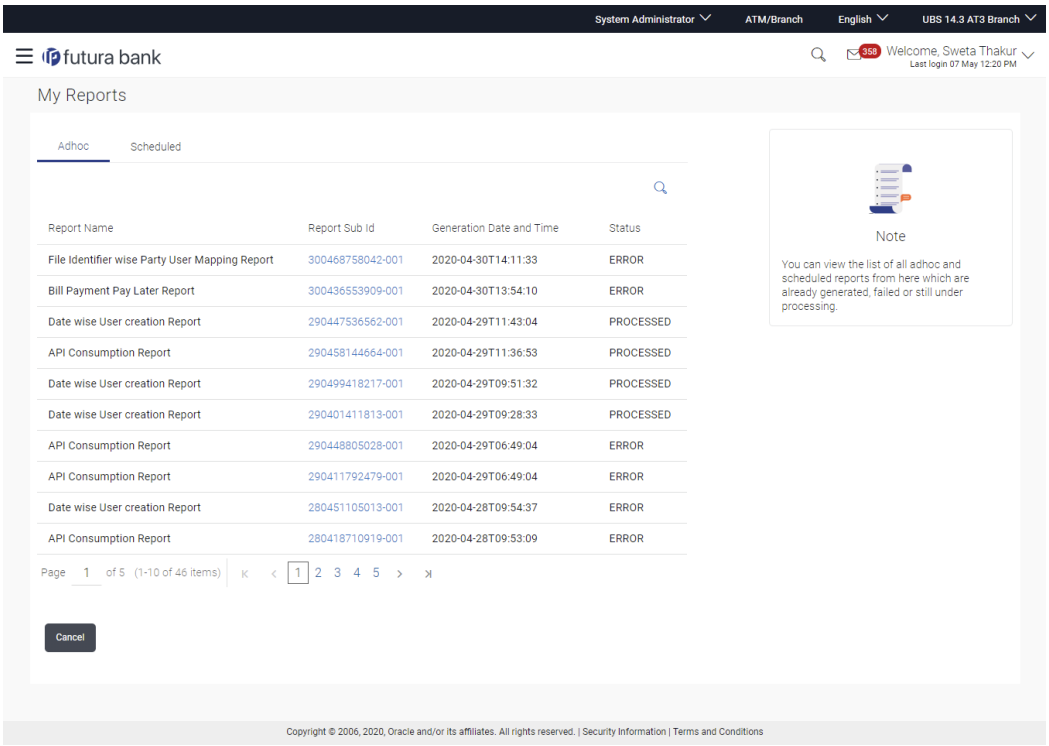
System/ Bank Administrator Dashboard > Toggle menu > Menu > Reports > My Reports

61.1 My Reports - Adhoc

Adhoc reports are generated on demand or on request. Generated reports can be viewed using ‘My Reports’ screen.

To view and download the generated adhoc reports:

My Reports - Adhoc



Field Description

Field Name	Description
Search	
Report ID	Report ID to search specific report. All the report IDs will be listed.
Report Name	Report Name to search specific report. All the reports with the names will be listed.
Generation Date	To search generated reports between specific date ranges. • From date – To search the reports generated from specific date. • To date – To search the reports generated till specific date
Report List	
Report Name	Report Name to search specific report. All the reports with the names are listed.
Report Sub Id	Report sub ID with the hyperlink to see the report details. .
Generation Date and Time	Report generation time and date.
Status	Status of generated reported. The status can be: • Processed • Pending • Error

1. Click search icon to search the reports with given search criteria. The search results matching to the search criteria are shown on the same screen.
2. Click on **Report Sub Id** hyperlink to view the detailed report. (Refer specimen provided for each report)

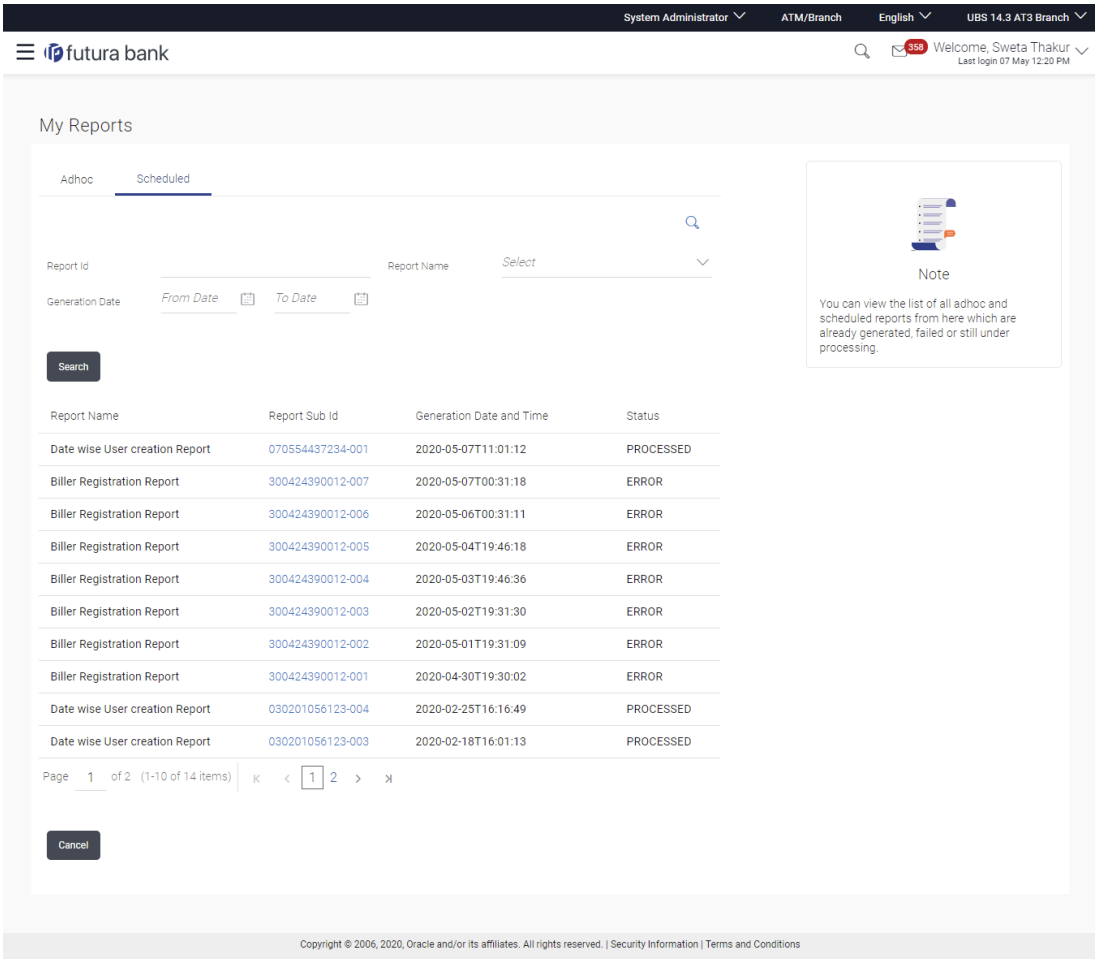
61.2 My Reports - Scheduled

The reports that are generated in specific time frame such as daily, weekly, monthly, quarterly, and annually are categorized under scheduled reports.

To view and download the generated scheduled reports:

1. Click the **Scheduled** tab. The list of scheduled reports appear.
   OR
   Click search icon to search the reports with given search criteria. The search results matching to the search criteria are shown on the same screen.

My Reports - Scheduled



Field Description

Field Name	Description
Search	
Report ID	Report ID to search specific report. All the report IDs will be listed.

Field Name	Description
Report Name	Report Name to search specific report. All the reports with the names will be listed.
Generation Date	To search generated reports between specific date ranges. • From date – to specify the date from which the generated reports to be searched. • To date – to specify the date till which the generated reports to be searched.
Report List	
Report Name	Report Name to search specific report. All the reports with the names will be listed.
Report Sub Id	Links of view the specific report.
Generation Date and Time	Report generation time and date.
Status	Status of generated reported. The status can be: • Processed • Pending • Error

2. Click on **Report Sub ID** hyperlink to view the detailed report. (Refer specimen provided for each report)

FAQ

1. **Can I choose a format in which a report is to be downloaded from My Reports screen?**

   A report can be downloaded in a format selected while generating a report.

2. **Can I view and download a report which is generated by other administrator users?**

   Yes, you can view and download the reports which are generated by other administrator users using **My Reports** screen.

62. User Report Mapping

The user report mapping maintenance will allow the Bank Administrators to map the report or set of reports to a specific business user. The business users can generate and view the reports of which they have an access to.

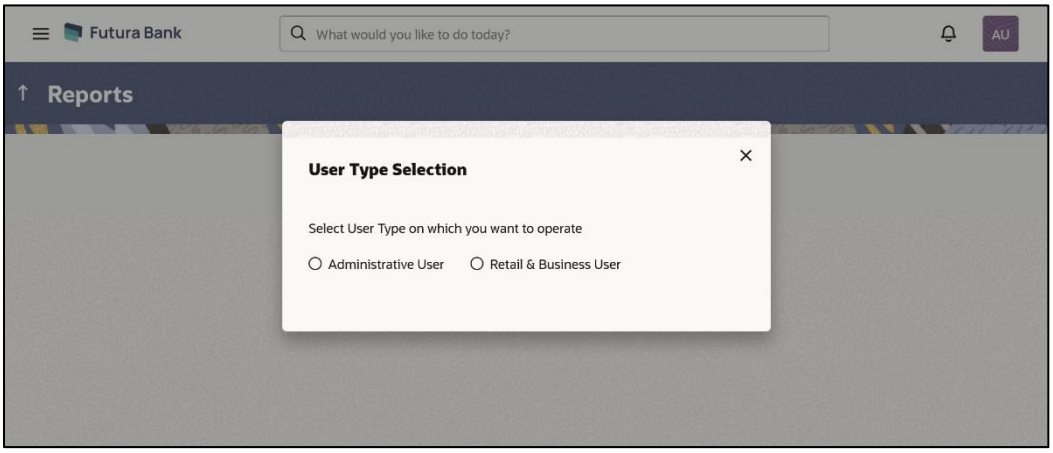
Bank Administrator can search a business user based on the user details and view the reports mapped to the user for each business party. Administrator can also un-map the reports from specific business user – Party combination so that access of the specific report/ s can be removed to that business user for a party. How to reach here:

System/ Bank Administrator Dashboard > Toggle menu > Menu > Reports > User Report Mapping

62.1 User Report Mapping – Select User Type

Bank Administrator logs into the system and navigates to the User Report Mapping screen. On accessing the 'User Report Mapping' menu, bank administrator has to select the user type for whom the reports are to be maintained.

User Report Mapping – Select User Type



3. Click **Administrator User** to map the report or set of reports to the bank administrator users. The **User Report Mapping - Administrator** screen appears.
4. Click **Retail and Business User** to map the report or set of reports to a specific business user. The **User Report Mapping - Retail and Business** screen appears.

62.2 User Report Mapping - Administrator User

62.2.1 User Report Mapping - Search

Using this option Bank Administrator can search and view the reports mapped to the user.

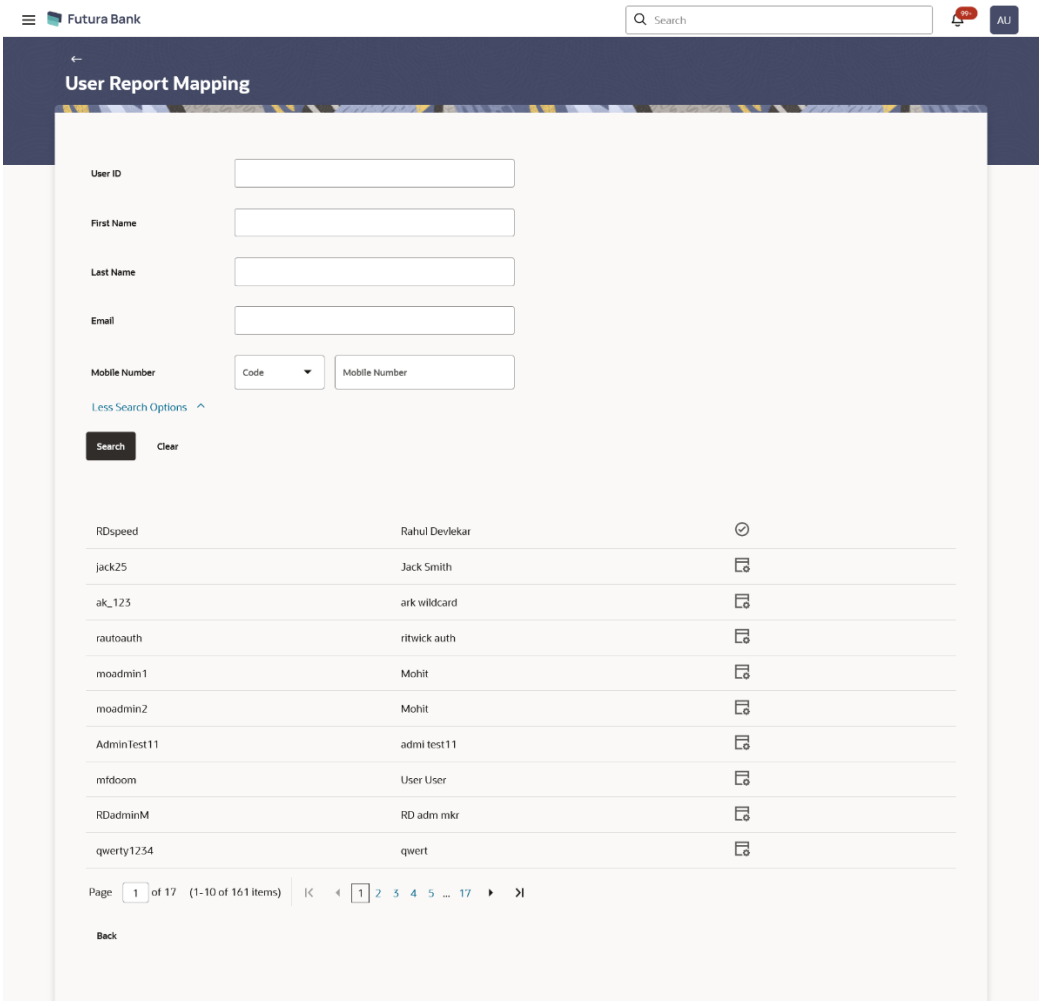
To search and view the reports mapping:

1. In the **Username** field, enter the username of the user whose report mapping to be done.
   OR
   In the **First Name** field, enter the first name of the user whose report mapping to be done.
   OR
   In the **Last Name** field, enter the last name of the user whose report mapping to be done.
   OR
   In the **Email** field, enter the email of the user whose report mapping to be done.
   OR
   In the **Mobile Number** field, enter the mobile number of the user whose report mapping to be done.

Note: Click on **More Search Options** to allows search based on more criteria.

2. Click **Search**. The **User Report Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction .

User Report Mapping - Search

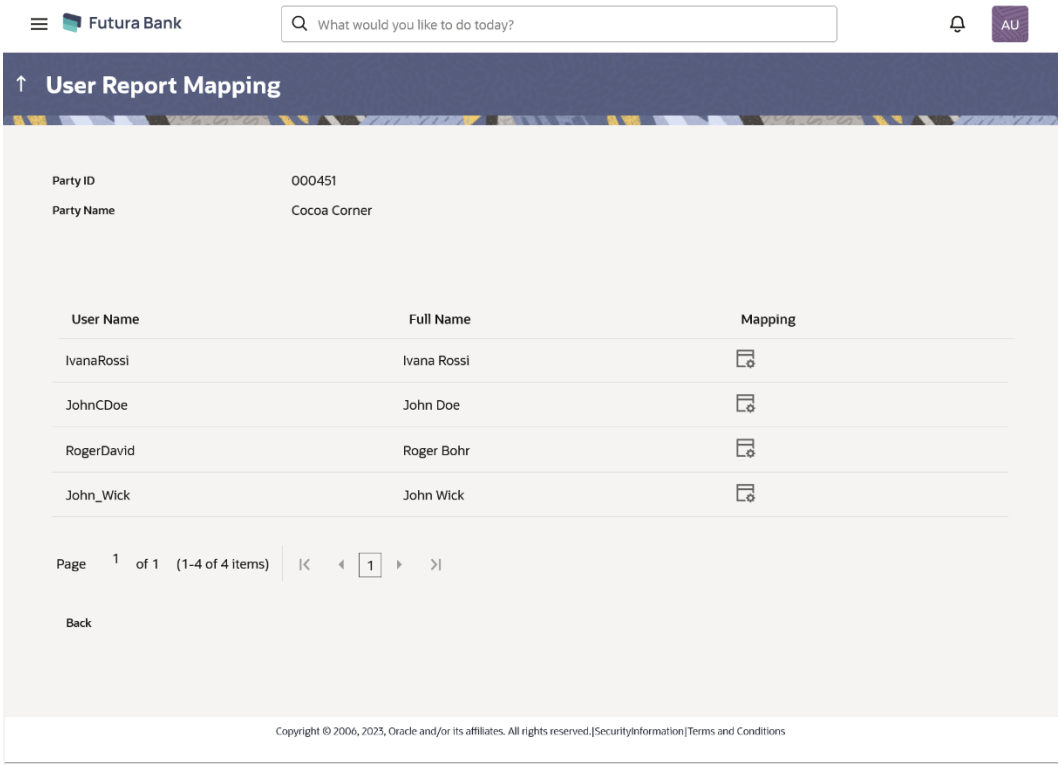


Field Description

Field Name	Description
Search Filter Criteria	
Username	Allows to search based on username of the user whose report mapping to be done.
First Name	Allows to search based on first name of the user whose report mapping to be done.
Last Name	Allows to search based on last name of the user whose report mapping to be done.
Email	Allows to search based on email ID by the user whose report mapping to be done.
Mobile Number	Allows to search based on mobile number of the user whose report mapping to be done. Note: User can select international subscriber dialing (ISD) code (country code) while selecting mobile number.
Search Result	
User Name	The name of the user.
Full Name	The full name of the user.
Mapping	Displays whether the file identifier is mapped to the user. • - denotes that the report is mapped to the user • - denotes that the report is not mapped to the user.

3. Click on the **Party ID** link to view the details. The **User Report Mapping - View** screen appears.

User Report Mapping - View

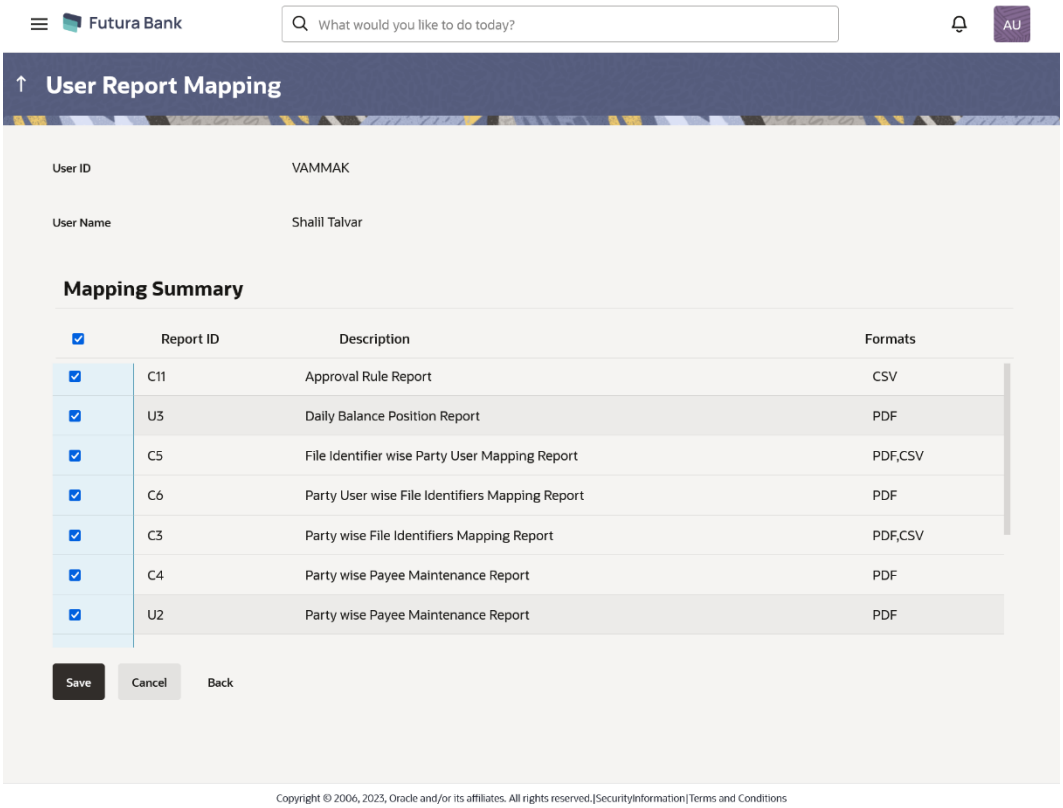


Field Description

Field Name	Description
Party ID	Party Id of the admin user.
Party Name	Party name of the admin user.
Users List	
User Name	The name of the user.
Full Name	The full name of the user.
Mapping	Displays whether the file identifier is mapped to the user. • - denotes that the report is mapped to the user • - denotes that the report is not mapped to the user.

4. Click against the user record for which you want to view the details. The **User Report Mapping – Mapping Summary** screen appears.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.

User Report Mapping – Mapping Summary



Field Description

Field Name	Description
User Name	Name of the admin user.
User ID	User Id of the admin user.
Mapping Summary	
Report ID	Unique id assigned to the mapped report.

Field Name	Description
Description	Description of the report.
Formats	Formats in which a report can be generated.

5. Click **Edit** to modify the user report mapping.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

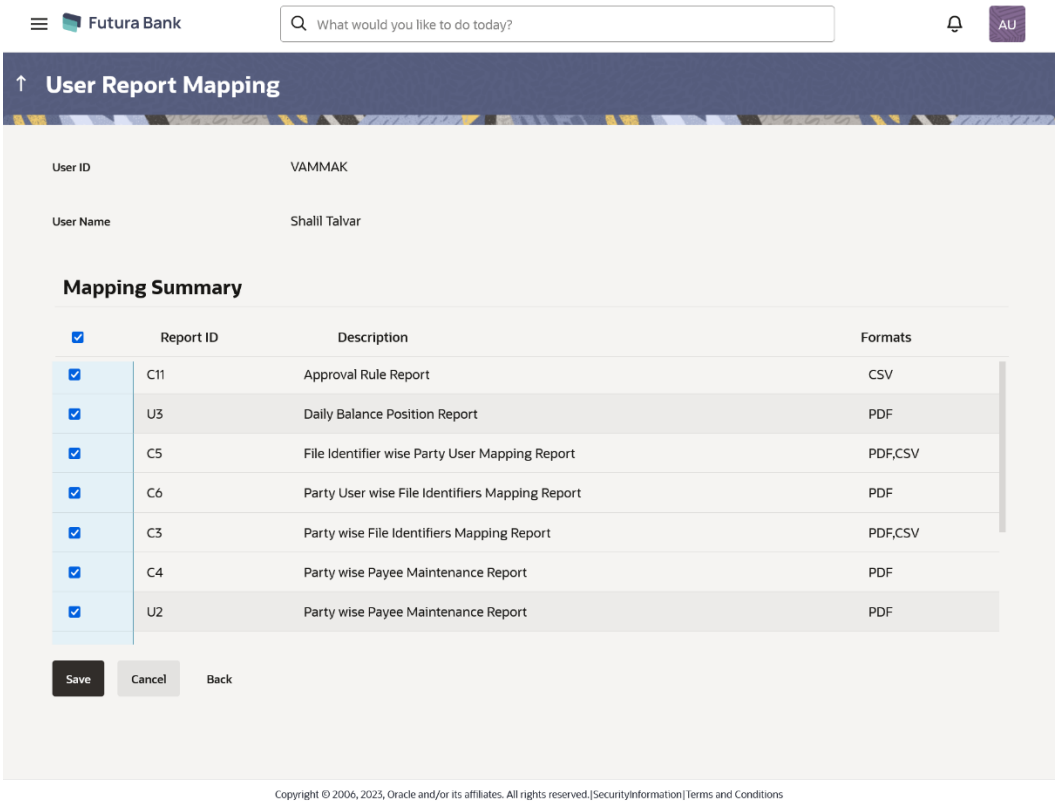
62.2.2 User Report Mapping - Create

Using this option Bank Administrator can map the reports to a specific corporate user.

To map the reports to a user:

1. In the **Username** field, enter the username of the user whose report mapping to be done.
   OR
   In the **First Name** field, enter the first name of the user whose report mapping to be done.
   OR
   In the **Last Name** field, enter the last name of the user whose report mapping to be done.
   OR
   In the **Email** field, enter the email of the user whose report mapping to be done.
   OR
   In the **Mobile Number** field, enter the mobile number of the user whose report mapping to be done.
2. Click **Search**. The **User Report Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.
3. Click of user record, for which you want to map the report/ s. The **User Report Mapping** screen to create the report mapping appears.

User Report Mapping - Create



Field Description

Field Name	Description
User Name	Name of the corporate user.
User ID	User Id of the corporate user.
Mapping Summary	
Report ID	Unique id assigned to a report.
Description	Description of the report.
Formats	The format in which the report is to be generated. The format could be PDF, XLSX.

4. In the **Mapping Summary** section, select the report id of the report which you want to map to the user.

5. Click **Save** to save the mapping.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
6. The **User Report Mapping - Review** screen appears. Verify the details and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
7. The success message appears along with the transaction reference number and status of the transaction.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

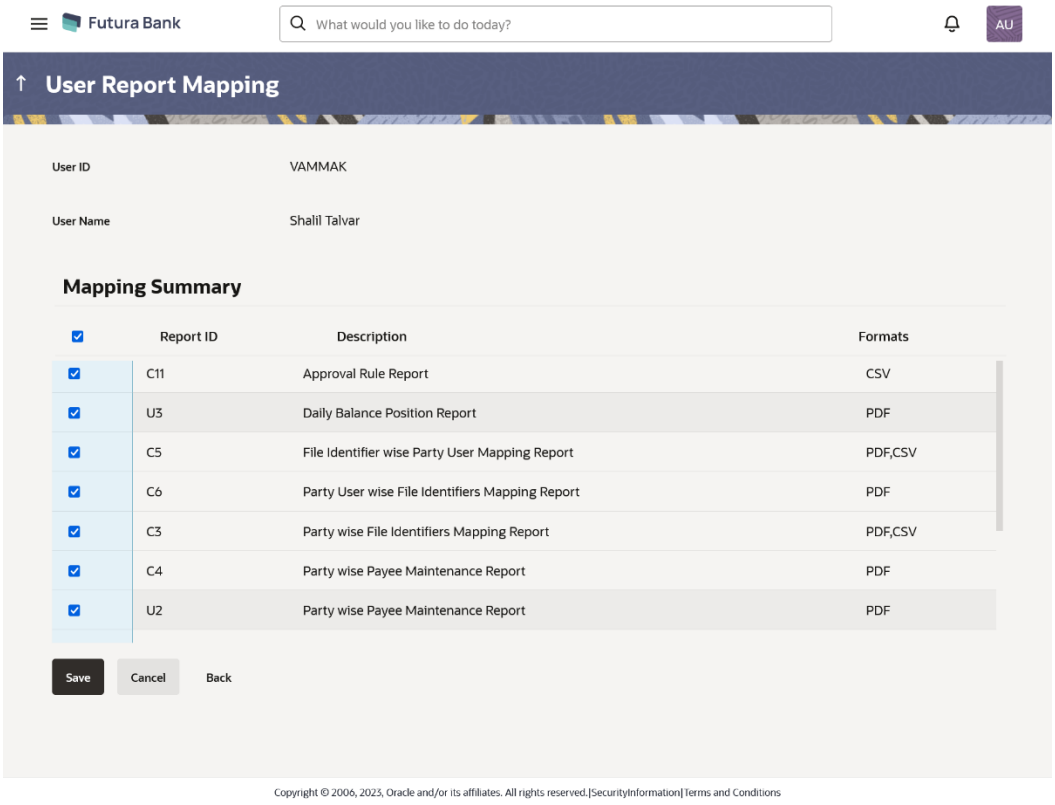
62.2.3 User Report Mapping - Edit

Using this option Bank Administrator can edit the mapping or un-map the reports from specific corporate user.

To edit a User Report Mapping:

1. In the **Username** field, enter the username of the user whose report mapping to be done.
   OR
   In the **First Name** field, enter the first name of the user whose report mapping to be done.
   OR
   In the **Last Name** field, enter the last name of the user whose report mapping to be done.
   OR
   In the **Email** field, enter the email of the user whose report mapping to be done.
   OR
   In the **Mobile Number** field, enter the mobile number of the user whose report mapping to be done.
2. Click **Search**. The **User Report Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.
3. Click against the file identifier record for which you want to view the details. The **User Report Mapping - View** screen appears.
4. Click **Edit**. The **User Report Mapping - Edit** screen appears.

User Report Mapping - Edit



5. View the details of report mapping already saved. Select or de-select the report id record to map / un-map a report to a user.
6. Click **Save** to save the modified details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
7. The **User Report Mapping - Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
8. The success message appears along with the transaction reference number and status of the transaction.
   Click **OK** to complete the transaction and navigate back to ‘Dashboard’.

62.3 User Report Mapping – Retail and Business User

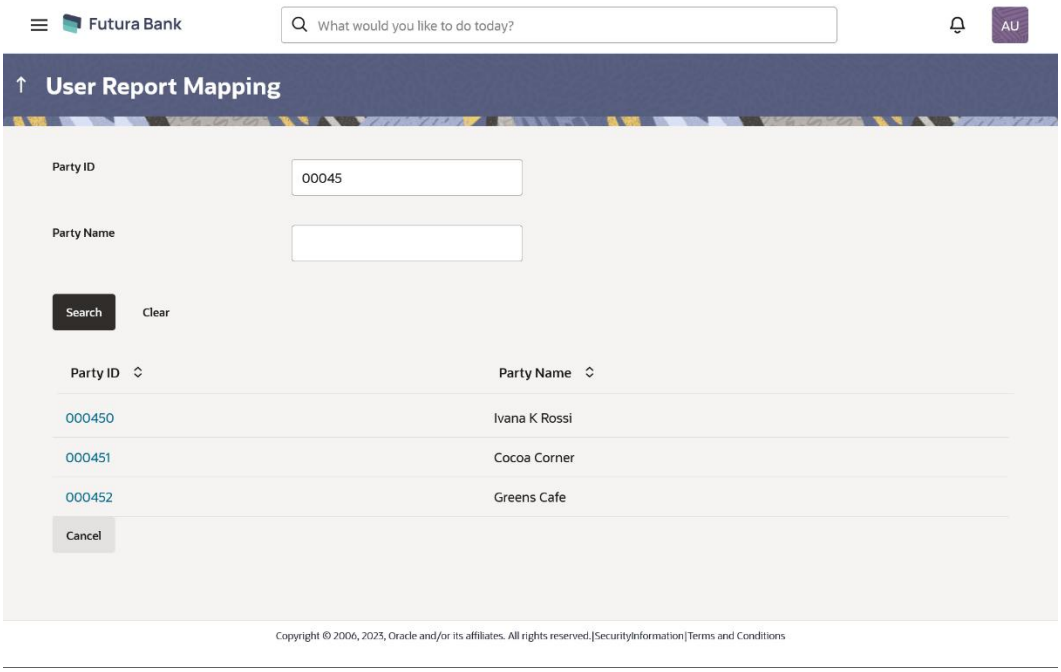
- Using this option Bank Administrator can search and view the reports mapped to the user. This option allows mapping a report or set of reports to a specific business user under a party.

62.3.1 User Report Mapping – Search and View

To search and view the reports mapping:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the name of the party.
2. Click **Search**. The **User Report Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.

User Report Mapping - Search

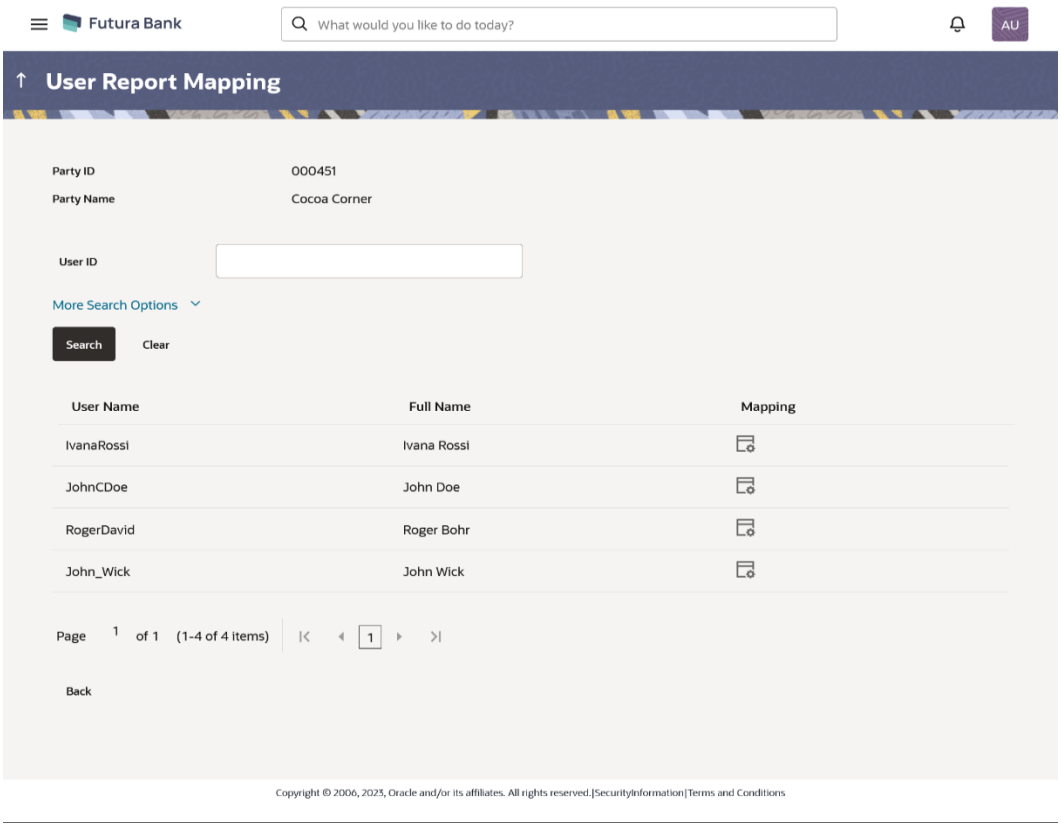


Field Description

Field Name	Description
Search Filter Criteria	
Party ID	Allows to search based on Party ID of the user whose report mapping to be done.
Search by Party Name	Click on the link to search by party name corresponding to the party ID.
Search Result	
Party ID	The ID of the searched party.
Party Name	The name of the searched party.

3. Click on the **Party ID** link to view the details. The **User Report Mapping - View** screen appears.

User Report Mapping - View

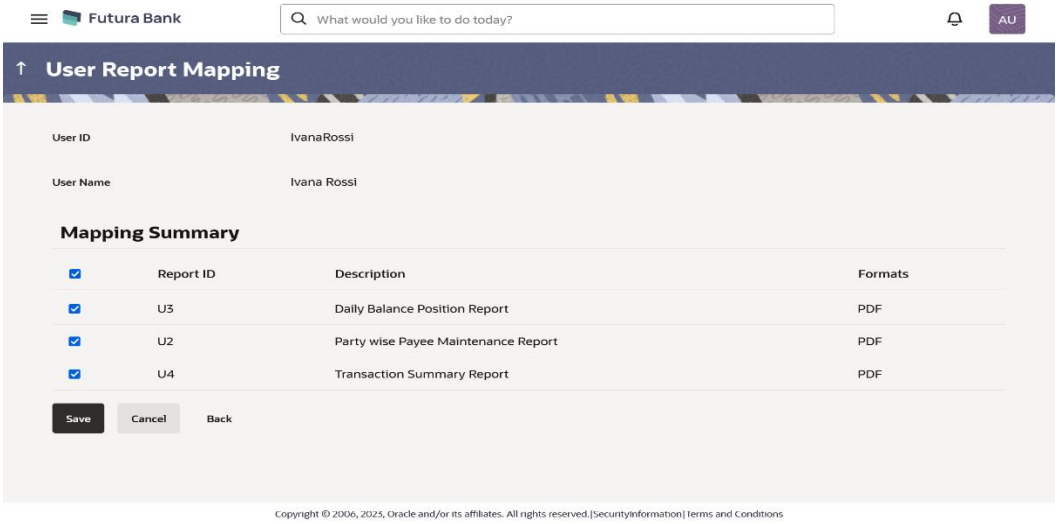


Field Description

Field Name	Description
Party ID	Party ID of the retail & business user.
Party Name	Party name of the retail & business user.
User ID	Allows to search based on ID of the user whose report mapping to be done.
Username	Allows to search based on username of the user whose report mapping to be done.
First Name	Allows to search based on first name of the user whose report mapping to be done.
Last Name	Allows to search based on last name of the user whose report mapping to be done.
Email	Allows to search based on email ID by the user whose report mapping to be done.
Mobile	Allows to search based on mobile number of the user whose report mapping to be done.
Users List	
User Name	The name of the user.
Full Name	The full name of the user.
Mapping	Displays whether the report mapping is done for the user or not. • - denotes that the report is mapped to the user • - denotes that the report is not mapped to the user.

4. Click against the user record for which you want to view the details. The **User Report Mapping – Mapping Summary** screen appears.
   OR
   Click **Back** to navigate to the previous screen.
   OR
   Click **Cancel** to cancel the transaction.

User Report Mapping – Mapping Summary



Field Description

Field Name	Description
User Name	Name of the retail & business user.
User ID	User Id of the retail & business user.
Mapping Summary	
Report ID	Unique id assigned to the mapped report.
Description	Description of the report.
Formats	Formats in which a report can be generated.

5. Click **Edit** to modify the user report mapping.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.

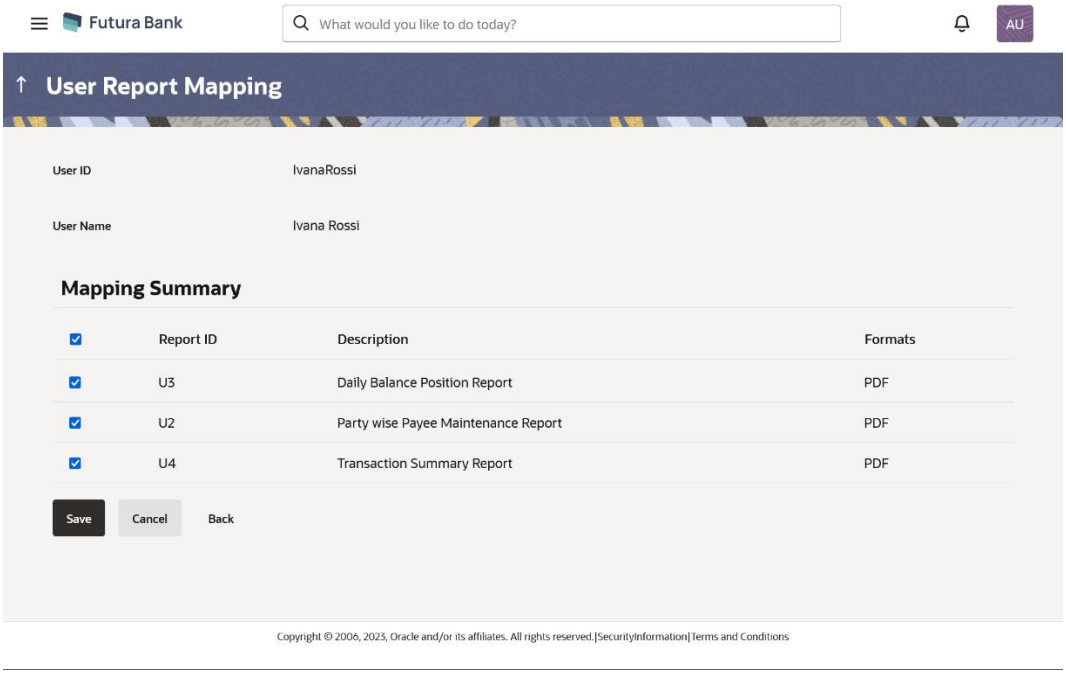
62.3.2 User Report Mapping - Create

Using this option Bank Administrator can map the reports to a specific corporate user.

To map the reports to a user:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the name of the party. In the **Username** field, enter the username of the user whose report mapping to be done.
2. Click **Search**. The **User Report Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.
3. Click of user record, for which you want to map the report/ s. The **User Report Mapping** screen to create the report mapping appears.

User Report Mapping - Create



Field Description

Field Name	Description
User Name	Name of the retail & business user.
User ID	User ID of the retail & business user.
Mapping Summary	
Report ID	Unique ID assigned to a report.
Description	Description of the report.
Formats	The format in which the report is to be generated. The format could be PDF.

4. In the **Mapping Summary** section, select the report id of the report which you want to map to the user.
5. Click **Save** to save the mapping.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
6. The **User Report Mapping - Review** screen appears. Verify the details and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to the previous screen.
7. The success message appears along with the transaction reference number and status of the transaction.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

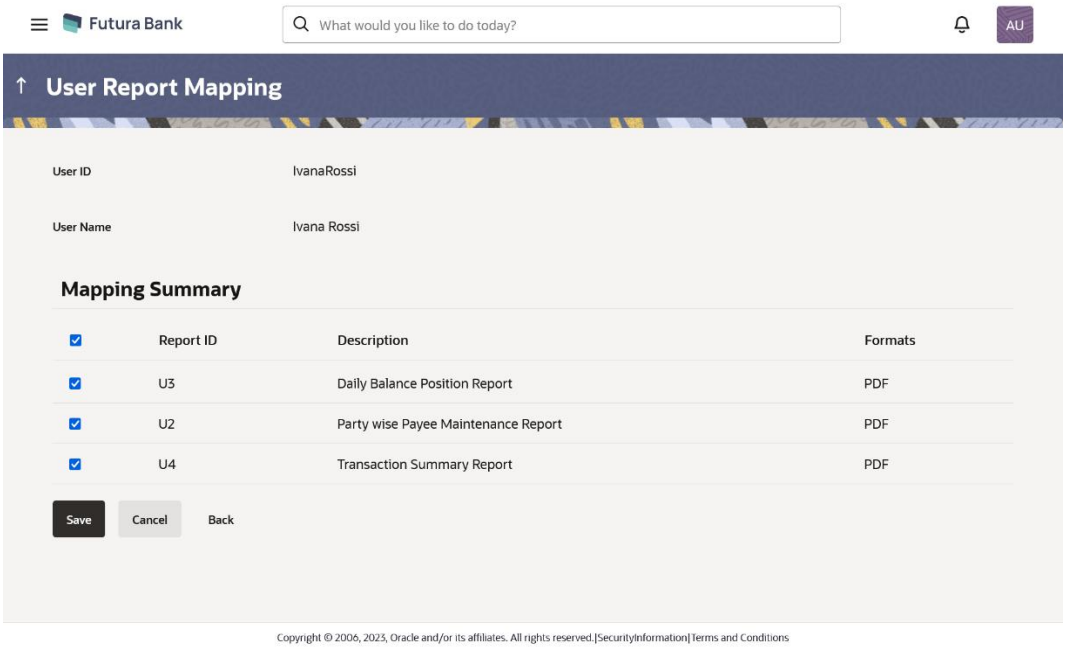
62.3.3 User Report Mapping - Edit

Using this option Bank Administrator can edit the mapping or un-map the reports from specific corporate user.

To edit a User Report Mapping:

1. In the **Party ID** field, enter the party id of the user.
   OR
   In the **Party Name** field, enter the name of the party. In the **Username** field, enter the username of the user whose report mapping to be done.
2. Click **Search**. The **User Report Mapping** screen with search results appears.
   OR
   Click **Clear** to clear the search parameters.
   OR
   Click **Cancel** to cancel the transaction.
3. Click against the file identifier record for which you want to view the details. The **User Report Mapping - View** screen appears.
4. Click **Edit**. The **User Report Mapping - Edit** screen appears.

User Report Mapping - Edit



5. View the details of report mapping already saved. Select or de-select the report id record to map / un-map a report to a user.
6. Click **Save** to save the modified details.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.

7. The **User Report Mapping - Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate to previous screen.
8. The success message appears along with the transaction reference number and status of the transaction.
   Click **OK** to complete the transaction and navigate back to ‘Dashboard’.

1. .

63. User Helpdesk

This feature will allow Bank administrator to create business user's session and perform the transaction requested by business user if he has forgotten his internet banking password or is unable to perform a transaction using his internet banking.

To authenticate the user, system will send an OTP to the customer and the same OTP needs to be communicated to the administrator user so that he can enter it on the screen to create user's session.

Note: OTP should be maintained as the second factor authentication for 'Create Helpdesk Session' event in Authentication setup.

How to reach here:

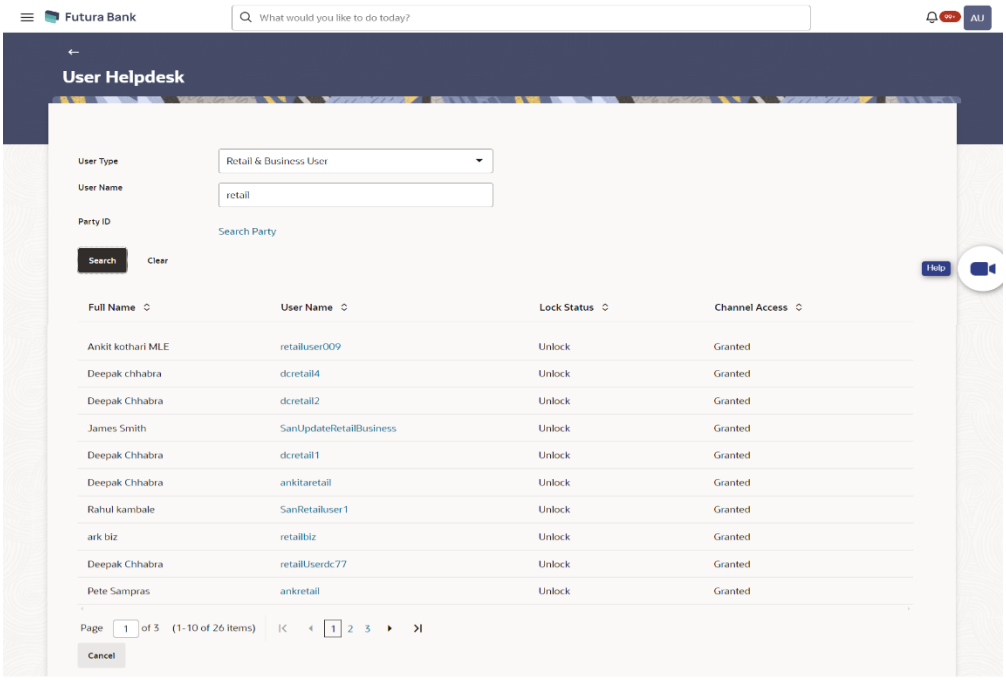
System/ Bank Administrator Dashboard > Toggle Menu > Menu > Others > User Helpdesk
OR
Bank Administrator Dashboard > Others > User Helpdesk

User Helpdesk - Search

To search user helpdesk:

1. From the **User Type** list, select the user.
2. In the **User Name** field, enter the name of the user.
   OR
   In the **Party ID** field, enter the party ID.
3. Click **Search**.

User Helpdesk - Search



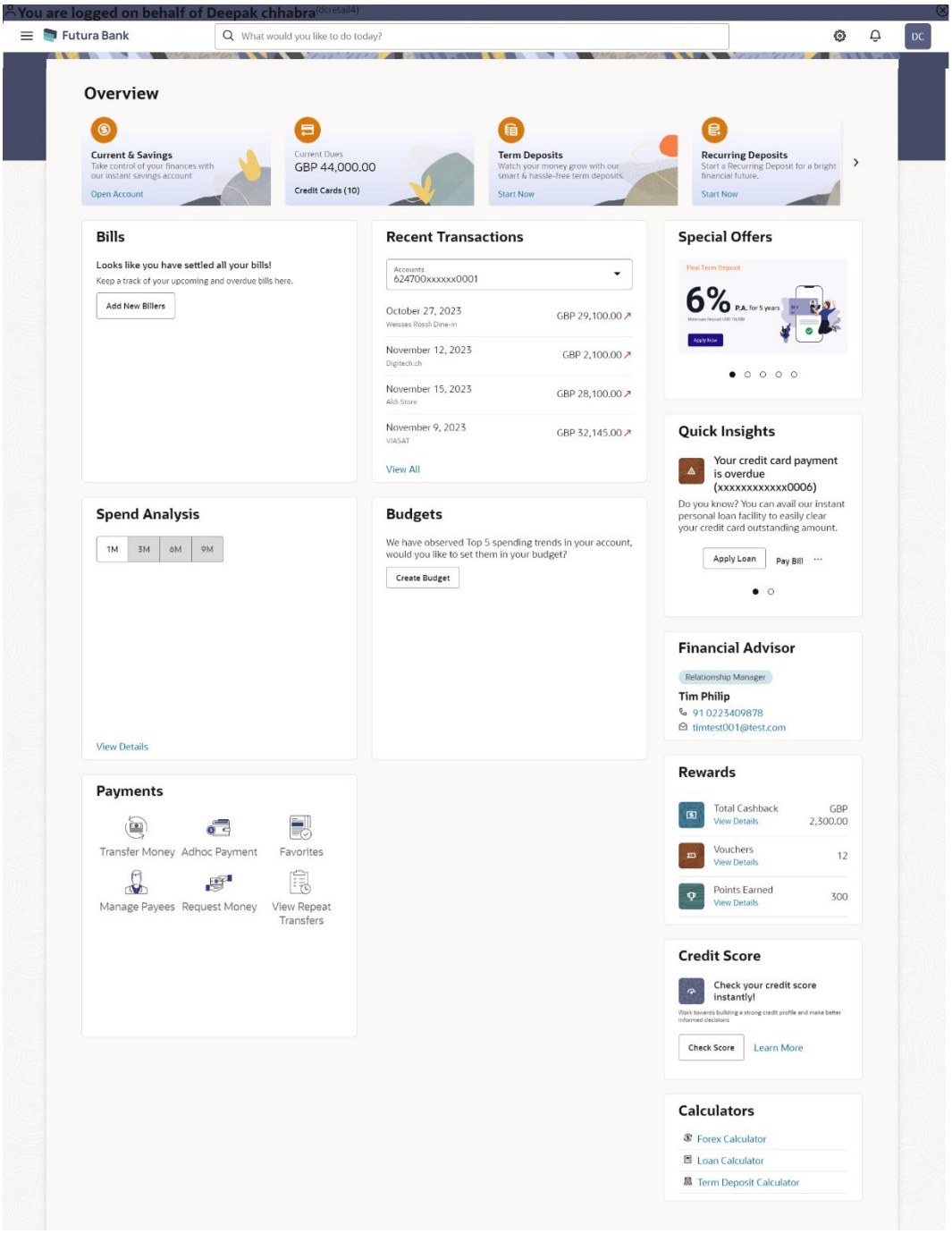
Field Description

Field Name	Description
User Type	The user type for which the help desk session has to be created.
User Name	User name (User ID) of the user for which help desk session has to be created.
Party ID	Party ID of the user for which the help desk session has to be created. Administrator can enter either the party ID or the user name.
Search Result	
Full Name	Displays the full name of the user.
User Name	Displays the user name (user ID) of the user.
Party ID	Displays the party ID of the user.
User Type	Displays the type of the user (Retail/Corporate).

4. Click on the **User Name**. Session of the selected user gets displayed.

User Helpdesk - Detail

The header displays the user name on behalf of whom the session is in progress. You can click icon to close the active session. Once the active session is successfully closed, the Administrator will be navigated to the Dashboard.



FAQ

1. **Can the Bank administrator create the helpdesk session for a new user (who has channel banking facility but has never logged in)?**

   No, for new users helpdesk session cannot be created, new users must login himself for the first time.

2. **Can the administrator set the 2FA mode anything else other than OTP for 'Create Helpdesk session' event in the Authentication screen?**

   System does not restrict the administrator from selecting a mode while setting up 2FA for 'Create Helpdesk session', however Administrator must set OTP as the 2FA mode for creating user helpdesk session.

3. **Can the administrator create the helpdesk session for the user, whose status is updated as 'Locked'?**

   No, the system will alert Bank Administrator to update the status of the user to "Unlock" from the User Management before creating the helpdesk session.

64. Mailbox

Mailbox is a two way communication channel between Bank customers and Bank administrators. Customers communicate with the bank via secured mailbox facility. Customers can send mail messages to the bank with specific pre-defined subjects for their queries/ complaints /feedback. In application, as day 0 maintenance each subject category is linked to a group of bank administrators' users. Depending upon the mail-subject mapping to each bank administrator user, administrators will receive the mails only of the subjects mapped to the users.

Administrators can view the number of received e-mails and access all received and sent e-mails from their secured mailbox. User can click the message to read the detailed content of the message. The subject of the message gives a brief understanding of what the message is about. User can view the message details, the sender information and also view the chain of messages exchanged if any.

The complete chain of message helps user to understand and know the information exchanged with the bank on a particular subject. Bank administrators can also view the alert messages sent by the bank on various banking events.

As a Day 0 maintenance, Bank has to define whether the OBDX mailbox should point to the UBS-interaction module or to the internal mailbox. In case if the mailbox is pointed to the UBS-Interaction module, the mail initiated by customers will be sent to the UBS bank user for his action and will not be sent to the OBDX administrator.

Pre-Requisites

- Roles and departments for various Bank Administrator must be defined in reference to mail section
- Alerts must be pre-set by bank and gets auto triggered if subscribed by customer or set as mandatory

Features supported in Application:

- **Inbox**: Where bank administrators can view the messages sent by the customers and also can reply and delete the mails.
- **Sent Mail folder:** This allows user to view the mails replied by logged in user. Also an option is provided to delete the mails.
- **Deleted Mail Folder:** This allows the user to view mails deleted from user's inbox and sent folders and can permanently delete the mails. There is an option to restore the deleted mails to respective folder.
- **Alerts:** View the alerts sent by the bank and received by logged in user. Also an option is provided to delete the alerts.
- **Notifications** - This section allows the logged in user to view all the notifications sent by the bank. Also an option is provided to delete the notifications.

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Mailbox > Mails
OR

System/ Bank Administrator Dashboard > Click

64.1 Mails

The following features are available under Mails:

- Inbox: This folder displays all the mail messages received by the user.
- Sent Mails: This folder displays the list of mail messages sent by the user to the bank.
- Deleted Mails: This folder contains the list of mail messages deleted by the user from the inbox and the sent mail folders.

How to reach here:

System/ Bank Administrator Dashboard > *Toggle Menu* > *Menu* > Mailbox > Mails
OR
System/ Bank Administrator Dashboard > > Click > Mails > View All

64.1.1 Inbox

Using this feature, the user can view the messages received in his Inbox. The user can view an individual message by clicking on the subject of the specific mail.

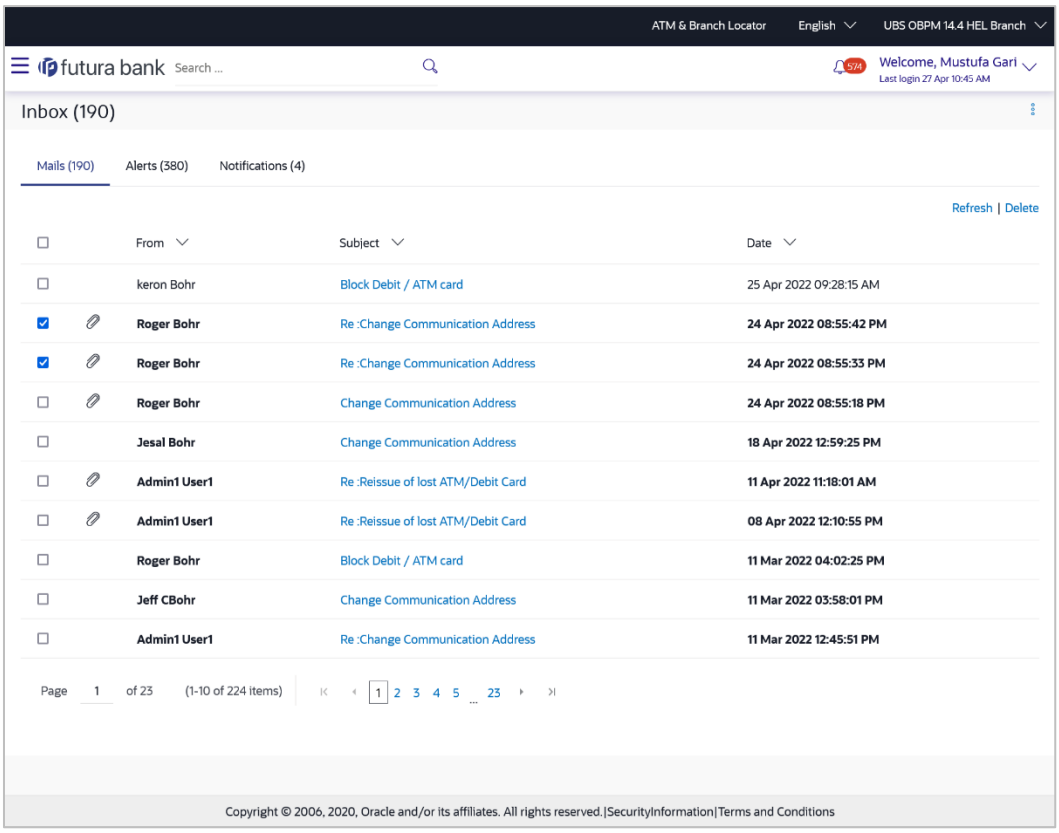
How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Mailbox > Mails > Inbox
OR
Access through the kebab menu of any other screens available under Mailbox

To view received mails:

1. The list of received messages appears on the **Inbox** screen. Click on the subject link of an individual message to view the details of that message.

Inbox



Field Description

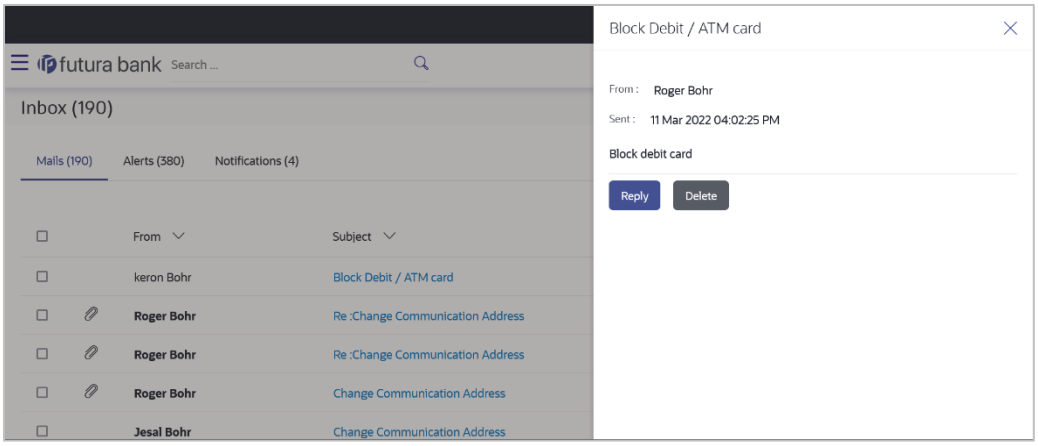
Field Name	Description
From	The name of the sender of the mail.
Subject	The subject of the mail is displayed against each mail record.

Field Name	Description
Date	The date and time on which the mail was received is displayed against each mail record.

To access the Inbox:

1. Click the subject of a mail you want to view. The mail details are displayed on the overlay window.
   OR
   Click **Refresh** to refresh the folder.
   OR
   To delete one or multiple messages, select the specific check boxes against the mail and click **Delete**.
   OR
   Click on kebab menu to access mailbox related transactions.

Inbox - Message Details



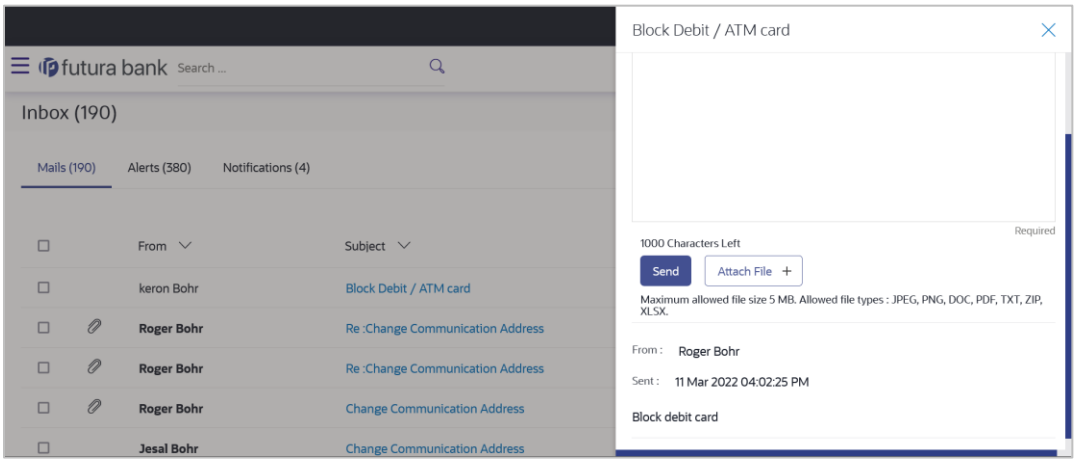
Field Description

Field Name	Description
Message Details	
Message Heading	The subject of the received mail.
From	The name of the sender of the mail.
Sent	The date and time on which the mail was received.
Content	The content of the mail.

Field Name	Description
Mail Chain	All the mails forming part of the mail chain being viewed are displayed one below the other with the mail received most recently displayed on top. Each mail in the chain contains the following: • The name or ID of the sender of the mail. Mails sent by you will have your name displayed against the From field and those sent by a bank administrator will have the ID of the bank administrator displayed. • The date and time at which the mail was sent. • The content of the mail as sent by you or the administrator. **Note**: A mail chain is formed when a user sends a mail to the bank and a bank administrator responds to the mail.

2. An overlay containing the details of the mail appears. Click **Reply** if you wish to respond to the mail.
   OR
   Click **Delete** to delete the message.
   OR
   Click ✕ icon to close the overlay window.

Inbox - Reply



Field Description

Field Name	Description
Message - Reply	

Field Name	Description
Message	Enter a response to be sent to the bank.
Attach File +	Browse and select the reference document file sent along with an email message. Note: Maximum allowed file size 5MB and allowed file types are JPEG, PNG, DOC, PDF, TXT, ZIP.

3. Click **Send** to send the response to the bank.
   A message confirming that the mail has been sent successfully appears.
   OR
   Click **Attach File +** to add an attachment to the response mail.

64.1.2 Sent Mail

This folder displays all the messages sent by the user to the bank.

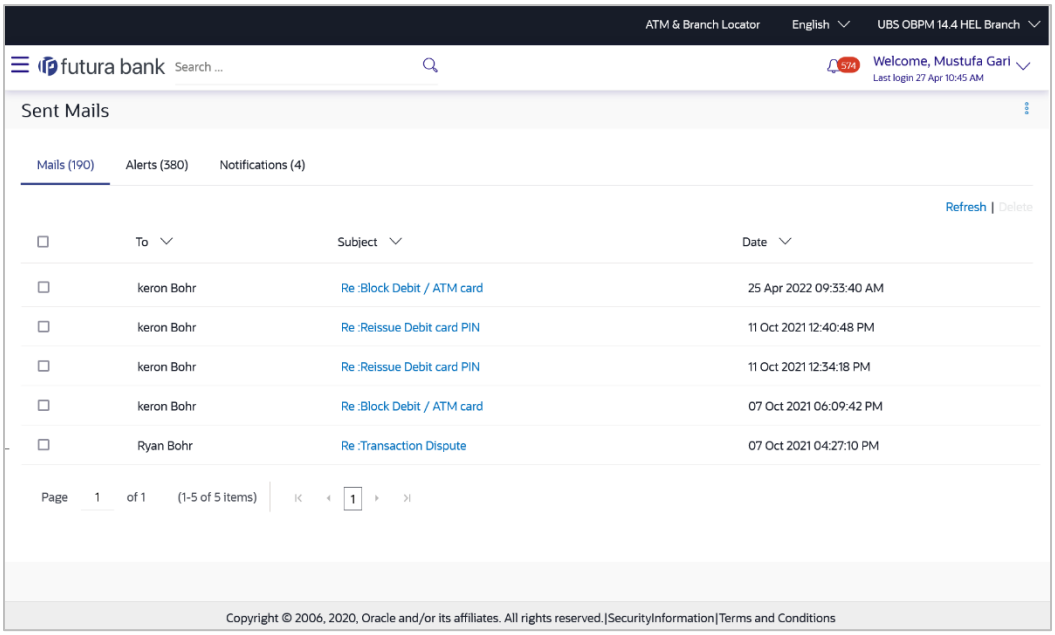
How to reach here:

Access through the kebab menu of transactions available under the Mailbox

To view the sent messages:

1. Click **Sent Mail**. The list of sent mails appears on the screen. Click on the subject link of an individual message to view the details of that message.

Sent Mail



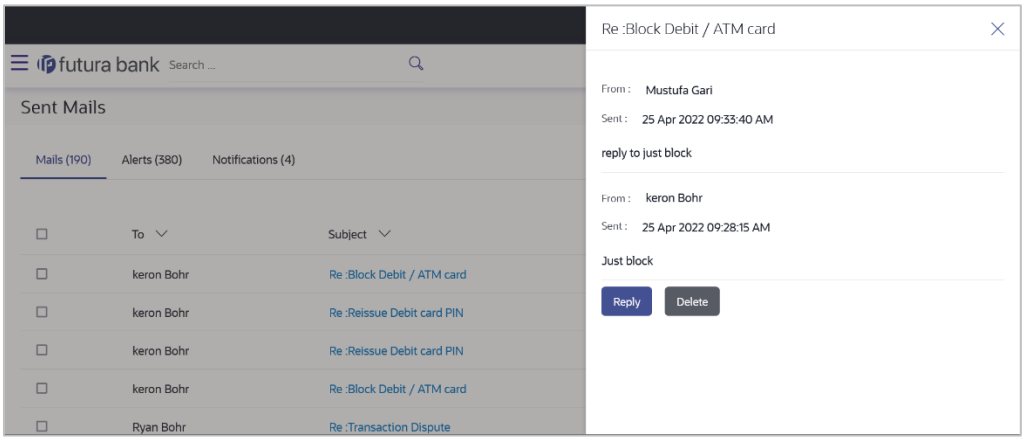
Field Description

Field Name	Description
To	The name of the receiver of the mail.
Subject	The subject of the mail is displayed against each mail record.
Date	The date and time on which the mail was sent is displayed against each mail record.

2. Click the link on the subject of the specific sent message that you wish to view.
   OR
   Click **Refresh** to refresh the mailbox.
   OR
   To delete a single or multiple mails, select the check box (s) against the mail, and click **Delete** to delete the message.
   OR
   Click on kebab menu to access other mailbox related transactions.
3. An overlay with details of the selected mail appears. Click **Reply** if you wish to respond further to the mail. Type the reply, and click **Send**. The success message appears.
   OR
   Click **Delete** to delete the message.

64.1.3 Sent Mails – Details

Sent Mail - Details



Field Description

Field Name	Description
Message Details This section displays the detailed message.	

Field Name	Description
Message Heading	The subject of the sent mail.
From	The name of the sender of the mail.
Sent	The date and time on which the mail was sent.
Content	The content of the mail.
Mail Chain	All the mails forming part of the mail chain being viewed are displayed one below the other with the mail received most recently displayed on top. Each mail in the chain contains the following: • The name or ID of the sender of the mail. Mails sent by you will have your name displayed against the **From** field and those sent by a bank administrator will have the ID of the bank administrator displayed. • The date and time at which the mail was sent. • The content of the mail as sent by you or the administrator. **Note**: A mail chain is formed when a user sends a mail to the bank and a bank administrator responds to the mail.

Message - Reply

This section will be displayed if you have selected the option **Reply**.

Message	Enter a response to be sent to the bank.

4. The overlay with details of the selected **Sent Mail** appears.
5. Click **Reply** if you wish to send a response to the bank.
   a. Type the reply and click **Send**. The success message appears.
      OR
      Click **Attach File** to add an attachment to the response mail.

   OR
   Click **Delete** to delete the message.
   OR
   Click ✕ to close the overlay window.

64.1.4 Deleted Mail

This folder displays all the messages that are deleted by the user from the Inbox and Sent Mail folders.

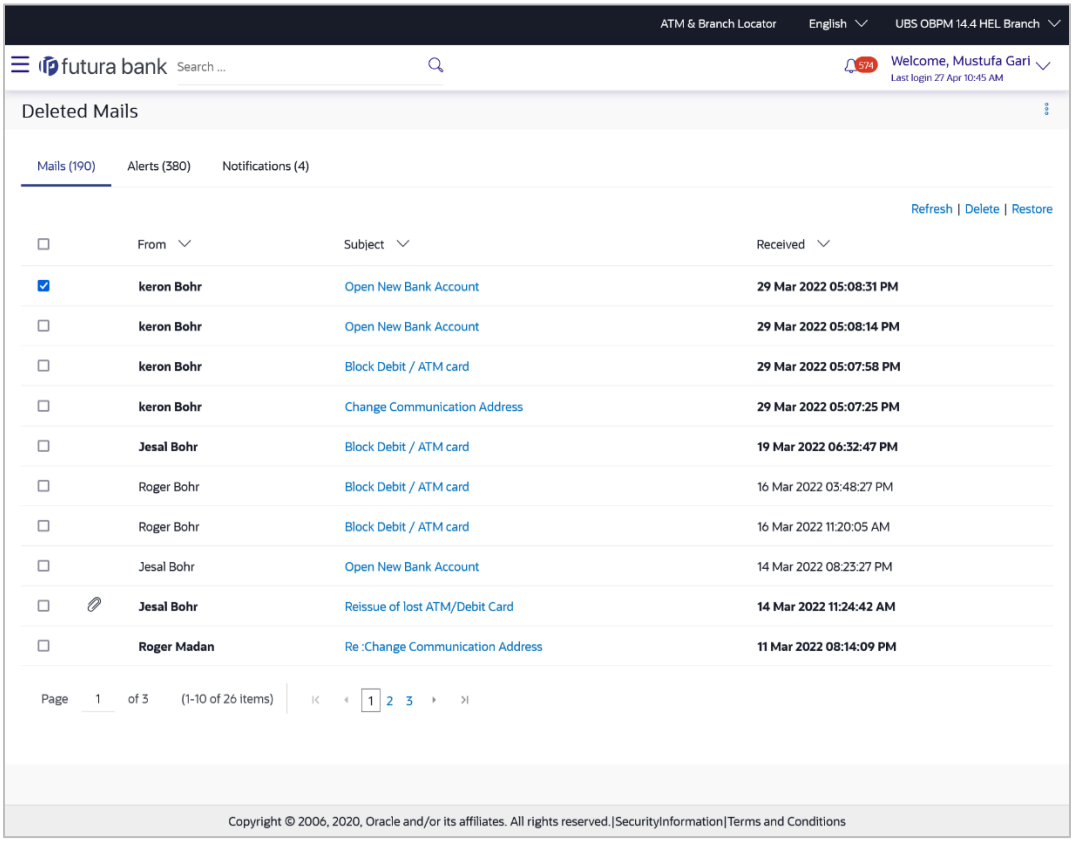
How to reach here:

Access through the kebab menu of transactions available under the Mailbox

To view the deleted messages:

1. The list of deleted messages appears on the screen. Click the link on the subject of any individual message to view the details of that message.

Deleted Mail



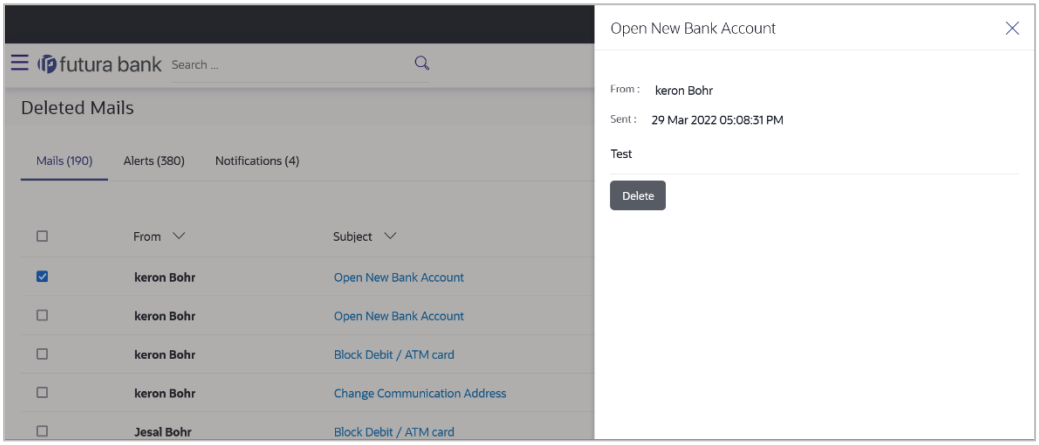
Field Description

Field Name	Description
From	The name of the sender of the mail.
Subject	The subject of the mail is displayed against each mail record.

Field Name	Description
Received	The date and time on which the message was sent/received is displayed against each mail record.

2. Click the subject link of the deleted message that you wish to view.
   OR
   Click **Refresh** to refresh the folder.
   OR
   To delete a single or multiple mails, select the check box (s) against the mail, and click **Delete** to delete the message/s.
   OR
   To restore the deleted mails back to inbox, select the check box(s) against the mail, and click **Restore**.
   OR
   Click on kebab menu to access mailbox related transactions.
3. The overlay screen on which details of the selected mail are displayed, appears.
   OR
   Click ✕ to close the overlay window.

Deleted Mail Details



Field Description

Field Name	Description
Message Details	
This section displays the detailed message.	
Message Heading	The subject of the deleted mail.
From	The name of the sender of the mail.
Sent	The date and time on which the message was sent/received.

Field Name	Description
Message Contents	The content of the deleted mail.

4. Click **Delete** to delete the message.
   OR
   Click ✕ to close the overlay window.

64.2 Alerts

Under this section, all the alerts auto generated and sent to the logged in user will be displayed. User is not allowed to reply to the alerts received in his mailbox. Number of unread mail count if any will be shown in this section.

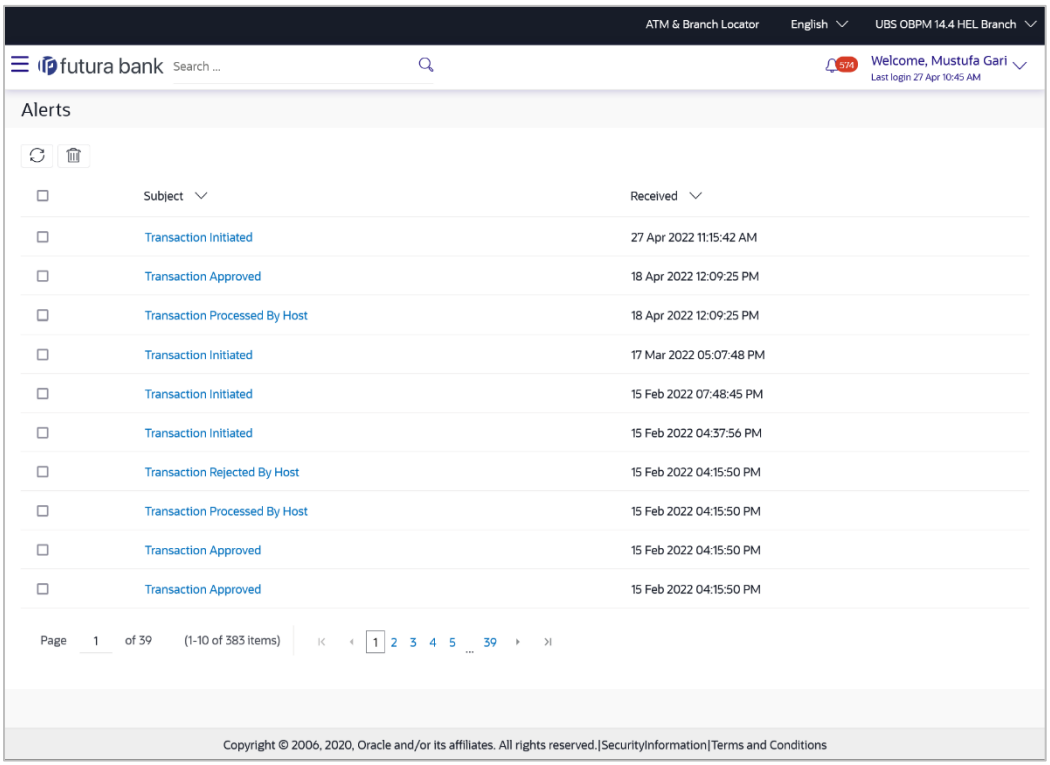
How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Mailbox > Alerts
OR
System/ Bank Administrator Dashboard > Click *> Alerts > View All*
OR
Access through the kebab menu of transactions available under the Mailbox

To view the alerts:

1. The alert screen appears.

Alerts



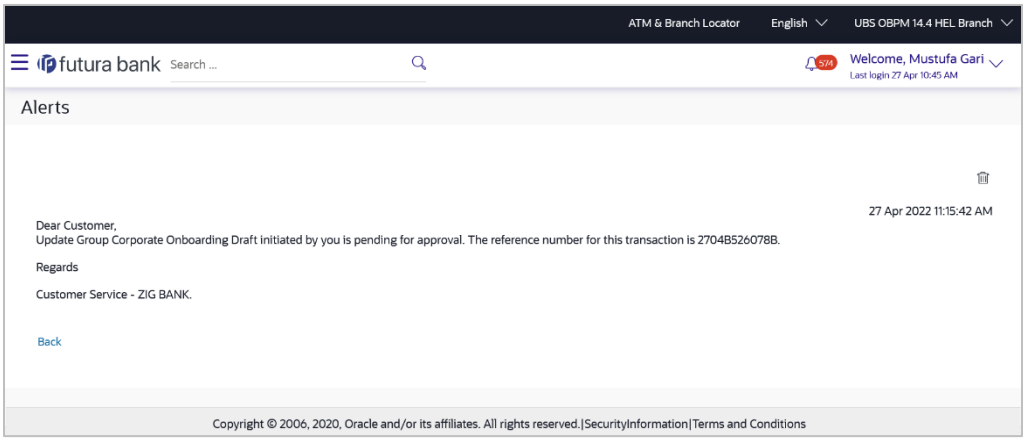
Field Description

Field Name	Description
Subject	The subject of the alert is displayed against the specific alert record.

Field Name	Description
Received	The date and time on which the alert was sent is displayed against the specific alert record.

2. Click an individual alert to view the details of the alert. The details of the alert appears.
   OR
   Click icon to refresh the mailbox.
   OR
   To delete multiple alerts, select the check box (s) against the alert, and click to delete the alert.

Alerts Details



Field Description

Field Name	Description
Alerts Details	
Received Date & Time	The date and time on which the alert was received.
Message	The content of the alert.

3. Click to delete the alert. The delete warning message appears.
   OR
   Click **Back** to navigate to the previous page.

64.3 Notifications

This section lists all the notifications sent to the logged in user will be displayed. The user can view the detailed notifications but cannot reply to these notifications. Number of unread notification count if any will be shown in this section.

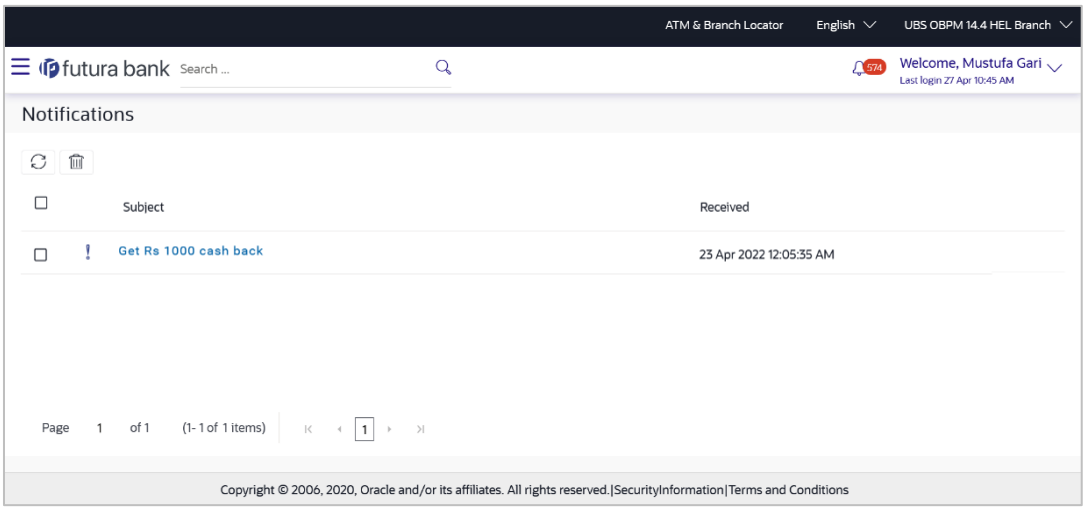
How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Mailbox > Notifications
OR
System/ Bank Administrator Dashboard > Click *> Notifications > View All*
OR
Access through the kebab menu of transactions available under the Mailbox

To view the notifications:

1. The **Notification** screen appears.

Notifications



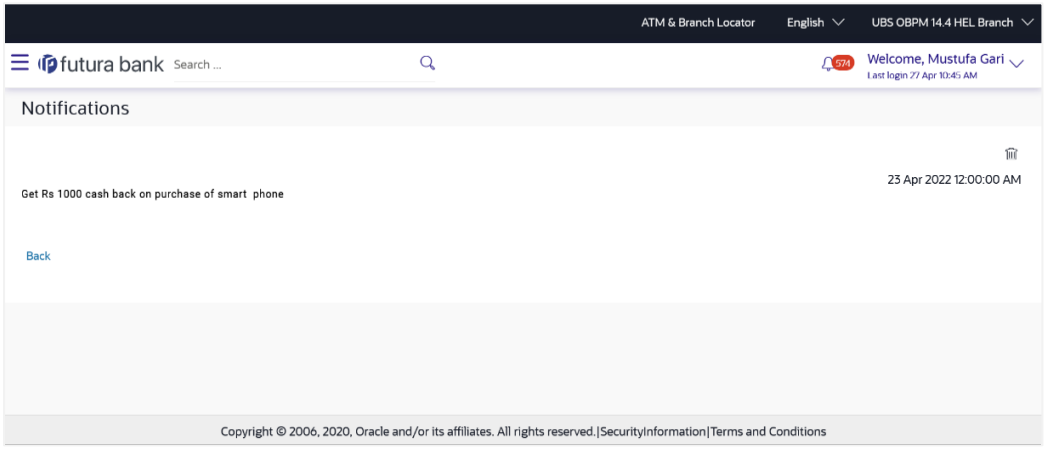
Field Description

Field Name	Description
Subject	The subject of the notification.
Received	The date and time on which the notification was received.

2. Click an individual notification to view the details of that notification. The screen on which the details of the notification are displayed appears.
3. Click icon to refresh the notifications.
   OR

   To delete multiple notifications, select the check box (s) against the notification, and click icon to delete the notification.

Notification Details



Field Description

Field Name	Description
Notification Details	
Received	The date and time on which the notification was received.
Message	The message body of the notification.

4. Click icon to delete the notification. The delete warning message appears.
   OR
   Click **Back** to navigate to the previous page.

FAQ

1. Can Bank Administrator initiate fresh mails?

No, Bank administrator can not initiate fresh mail. Administrator will be allowed only to reply to the mails received in their inbox.

2. Will Bank Administrators receive all mails initiated by bank's customers?

Bank Administrators will receive only those mails of which the mail subject is mapped to individual user or group of users. E.g. Mail initiated by customer with subject 'Change of communication address' will only be sent to the users whom this subject is mapped.

3. Can Bank Administrator view reply sent by other Administrator to customer's mail?

Yes, bank administrators can view the mails replied by other administrators, only if the mail subject is mapped to the user.

4. **Can Bank Administrator delete multiple mails?**

   Yes, user can select multiple mails and delete the same.

5. **Can Bank Administrator restore the deleted mails?**

   Deleted mails from inbox and sent mail folder will be stored in Deleted Mails folder. User can view the details of deleted mail and can restore the mail back in respective folders. Mails will get permanently deleted from user's view if further deleted from 'Deleted Mail folder'.

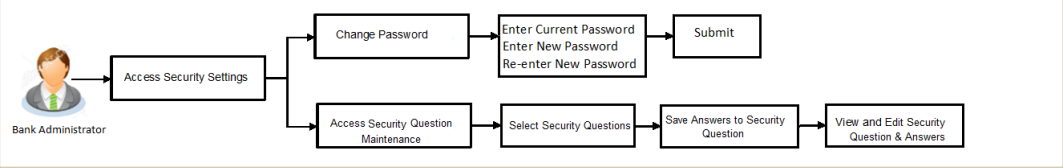
65. Security Settings

Security settings includes changing of password and setting of security questions for the user.

Pre-requisites

- User must have a valid Login credentials
- Transaction access is provided to Bank Administrator

Workflow



Features supported in application

The Security Settings maintenance allow the Bank Administrator to:

- Changing of old password to new Password
- Set Security Questions
- View Security Questions
- Edit Security Questions

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Security & Login

65.1 Set Security Question

Security Questions are the second layer of authentication mode set by the Bank to complete various transactions.

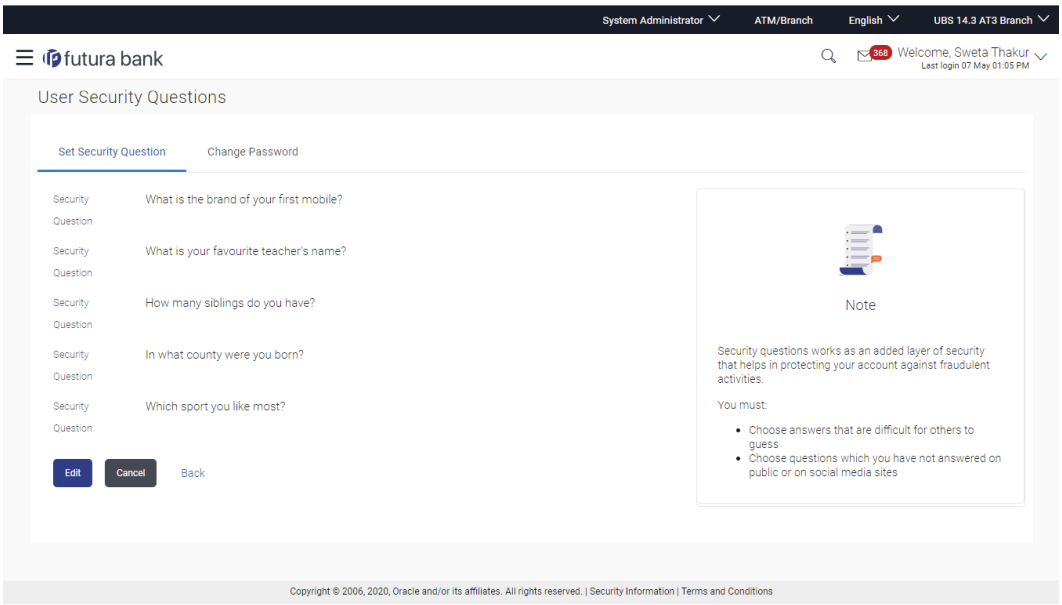
This feature allows the administrator user to set up the answers of the security questions, which will then be used as another layer of security (Over and above the Login credentials).

User will be asked to answer these security questions to complete the transactions for which bank would have set Security Question as the second factor authentication.

How to reach here:

Administrator Dashboard > Toggle Menu > Menu > Security & Login > Set Security Question

Set Security Question

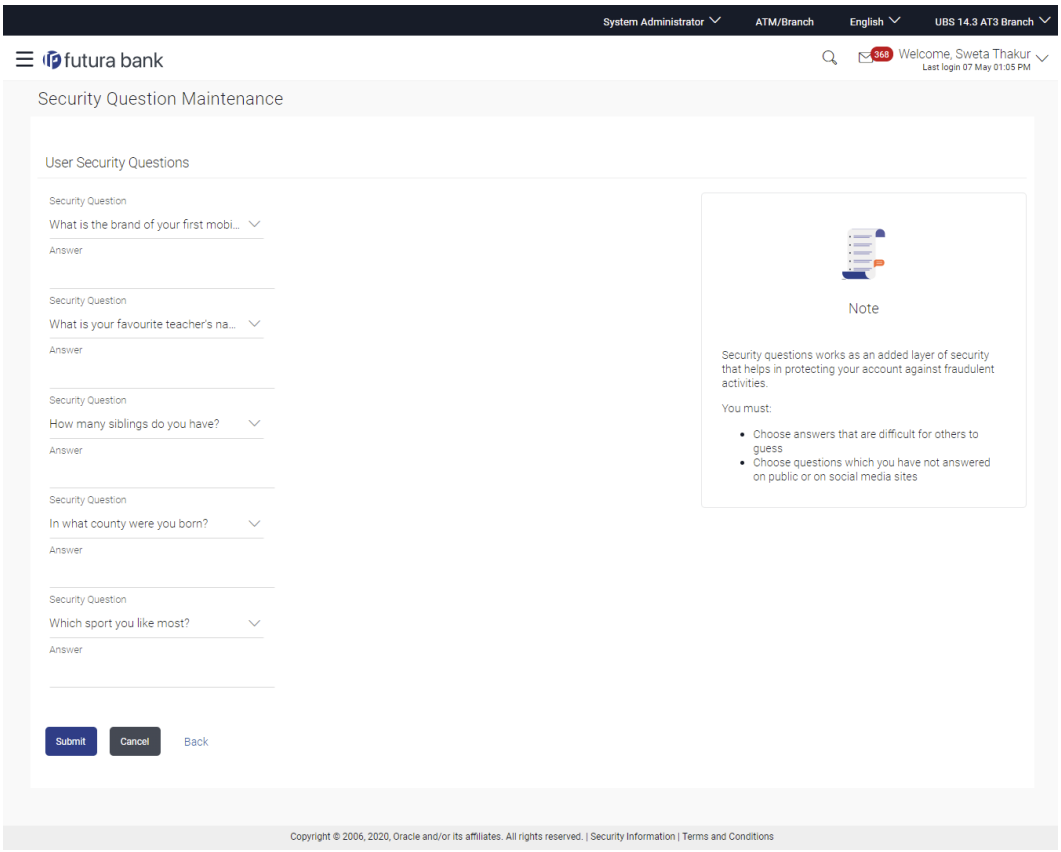


To set up security questions:

Note: Since security questions have not been set-up by the user, message will be displayed "Security Questions are not set up yet".

1. Click **Set up now** to set-up security questions. The **User Security Question** screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to '**Dashboard**'.
   OR
   Click **Back** to go back to the previous screen.

User Security Question



Field Description

Field Name	Description
User Security Questions	
Security Question	Questions available for selection for setup.
Answer	Enter the answers corresponding to the security question.

2. From the **Security Questions** list, select the appropriate security question to be added in set.
3. In the **Answers** field, enter the answers corresponding to the security question.
4. Click **Save** to save the changes made.
   OR
   Click **Cancel** to cancel the operation and navigate back to '**Dashboard**'.
   OR
   Click **Back** to go back to the previous screen.
5. The **User Security Question – Review** screen appears. Verify the details, and click **Confirm**.
   OR

Click **Cancel** to cancel the operation and navigate back to '**Dashboard'**.
OR
Click **Back** to make the changes if any.
The **User Security Question – Edit** screen with values in editable form screen appears

6. The success message appears along with the status of transaction.
   Click **OK** to complete the transaction and navigate back to '**Dashboard'**.

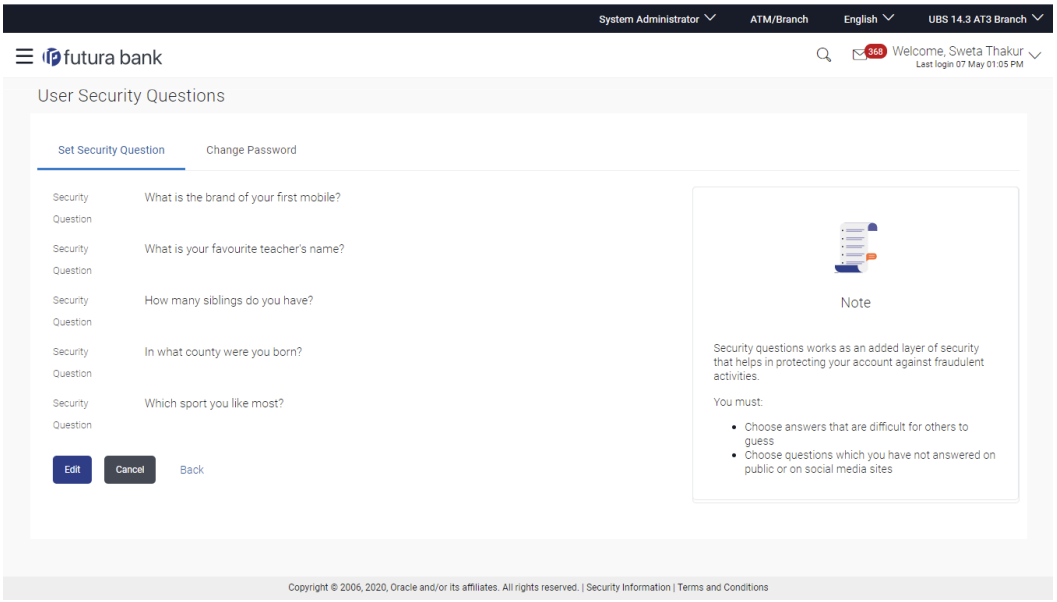
65.1.1 View Security Questions

On accessing 'Manage Security Questions' option, system displays the existing security questions already maintained if any.

To view the existing t security questions maintenance:

1. Navigate to **Set Security Question** screen, **Set Security Question - View** screen appears.

Set Security Question - View



Field Description

Field Name	Description
Set Security Question - View	
User ID	User ID of the logged in user.
Security Questions	The list of security question, which is the existing set, for the user

2. Click **Edit** to make the changes if any. The **User Security Question – Edit** screen with values in editable form appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to '**Dashboard**'.
   OR
   Click **Back** to go back to previous screen.

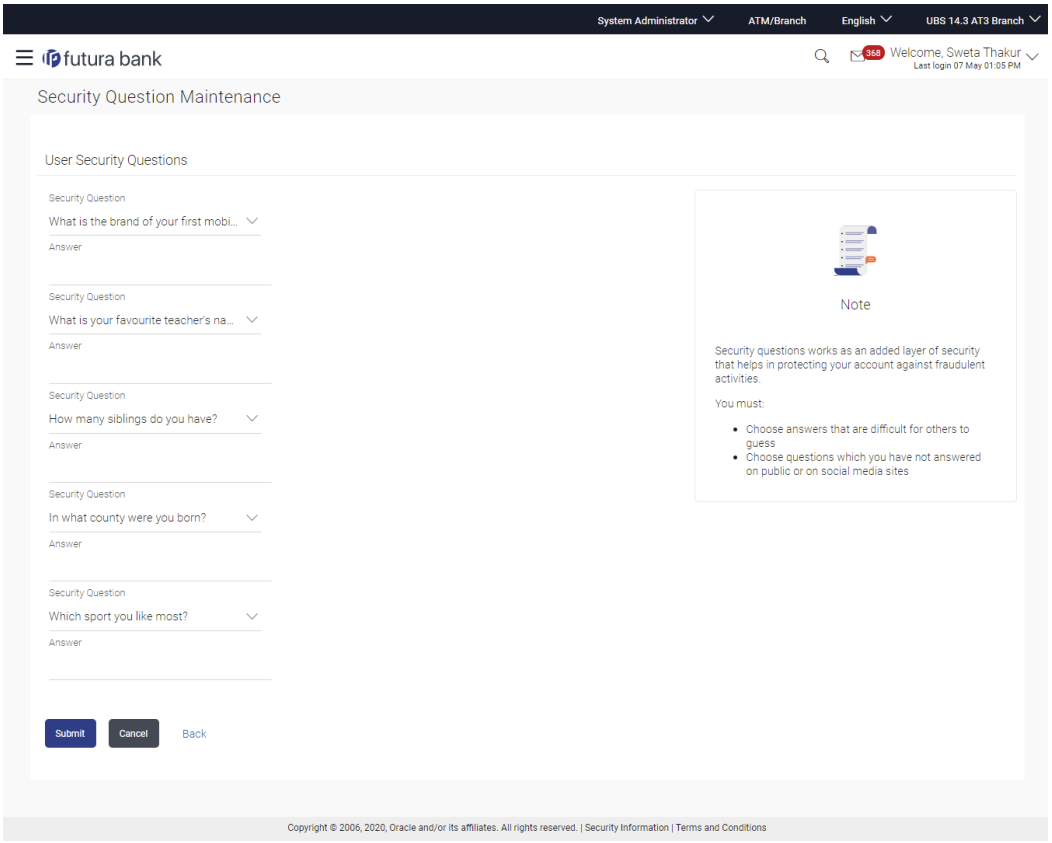
65.1.2 User Security Question - Edit

Bank Administrator can modify existing maintenance for security questions. Administrator is allowed to add security questions but cannot delete the existing questions.

To edit the security questions set:

1. Click **View** to view the security questions already set. The **User security questions – View** screen appears.
2. Click **Edit**. The **User Security Question - Edit** screen with values in editable form screen appears.

User Security Question - Edit



Field Description

Field Name	Description
User Security Question - Edit	
Questions	The list of security question, which is the existing set, for the user.
Answer	Answers will not be visible in edit mode due to security reasons.

3. From the **Security Questions** list, view the existing questions. Modify if required.
4. In the **Answers** field, enter the answers corresponding to the security question.
5. Click **Save** to save the changes made.
   OR
   Click **Cancel** to cancel the operation and navigate back to '**Dashboard**'.
   OR
   Click **Back** to go back to the previous screen.
6. The **User Security Question– Review** screen appears. Verify the details, and click **Confirm**.
   OR
   Click **Back** to make the changes if any.
   OR
   Click **Cancel** to cancel the operation and navigate back to '**Dashboard**'.
7. The **User Security Question – Edit** screen with values in editable form screen appears.
   OR
   Click **Cancel** to cancel the operation and navigate back to '**Dashboard'**.
   The success message of security question setup appears along with the transaction reference number.
   Click **OK** to complete the transaction and navigate back to 'Dashboard'.

66. Profile

Using this option, the bank administrator can view his profile details. Details that can be viewed include user name, last login time, email id, phone number, and date of birth and address of the user.

Pre-requisites

User must have a valid Login credentials

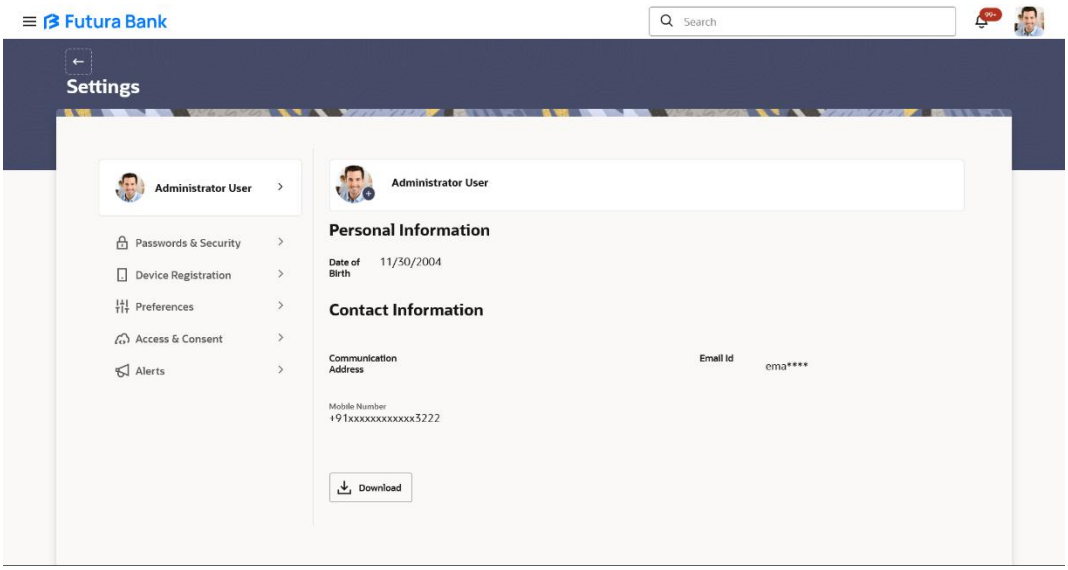
Features Supported In Application

- View the profile details of bank administrator user

How to reach here:

System/ Bank Administrator Dashboard > Toggle menu > Menu > Account Setting > Profile
OR
User Name icon (top right corner of the screen) > Profile

Profile



Field Description

Field Name	Description
User Name	First name and last name of the logged in user.
Personal Information	
Date of Birth	Date of birth of the user.

Field Name	Description
Contact Information	
Communication Address	Address of the user.
Email	Email id of the user, in masked format.
Phone Number	Displays contact number of the user alongwith an international subscriber dialing (ISD) code in masked format.

1. Click **OK** to navigate to the previous screen.

FAQ

1. Can the bank administrator user edit his profile information?

No, the bank administrator user cannot edit his profile information; he/she can only view the profile details.

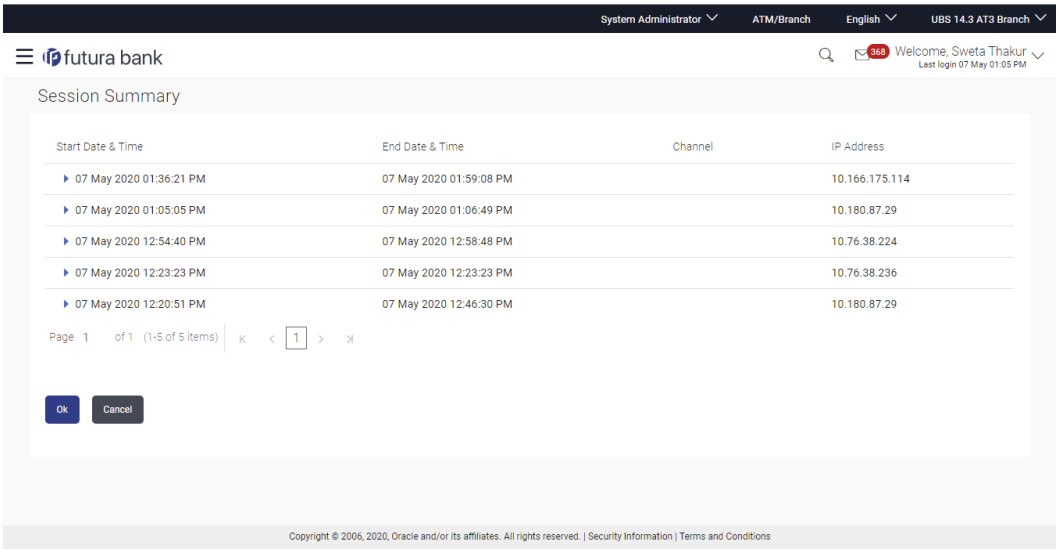
67. Session Summary

The option used by the user to check the log of transactions and login details for the previous five logins. The System Administrator can view the entire session summary of the previous five logins, login and logoff date and time for each session, channel in which transactions are carried out in each session along with the IP address of the channel.

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Account Settings > Session Summary

Session Summary

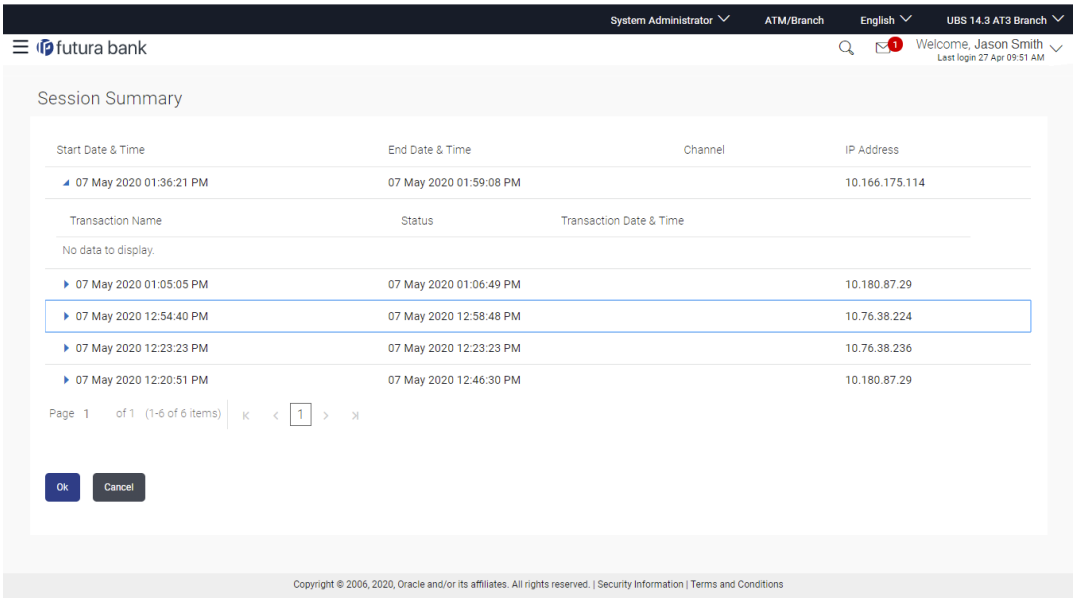


Field Description

Field Name	Description
Start Date & Time	The start date and time of the session.
End Date & Time	The end date and time of the session.
Channel	The channel of access for the session (Desktop Browser).
IP Address	IP address of the channel.

1. Click against a specific record to view the details of that session. The session details appear.
   OR
   Click **OK** to navigate to the Dashboard screen.

Session Summary - Details



Field Description

Field Name	Description
Start Date & Time	The start date and time of the session.
End Date & Time	The end date and time of the session.
Channel	The channel of access for the session (Desktop Browser).
IP Address	IP address of the channel.
Session Summary - Details	
Transaction Name	Name of the transaction, performed in the session.
Status	Status of the transaction.
Transaction Date & Time	The date and time of the transaction.

68. Manage DND Alerts

This option allows user to enable/disable do not disturb (DND) flag for mandatory alerts for the selected categories. Day 0 configuration is provided for the events which are applicable for DND. The bank can create a category of events for which DND needs to be configured.

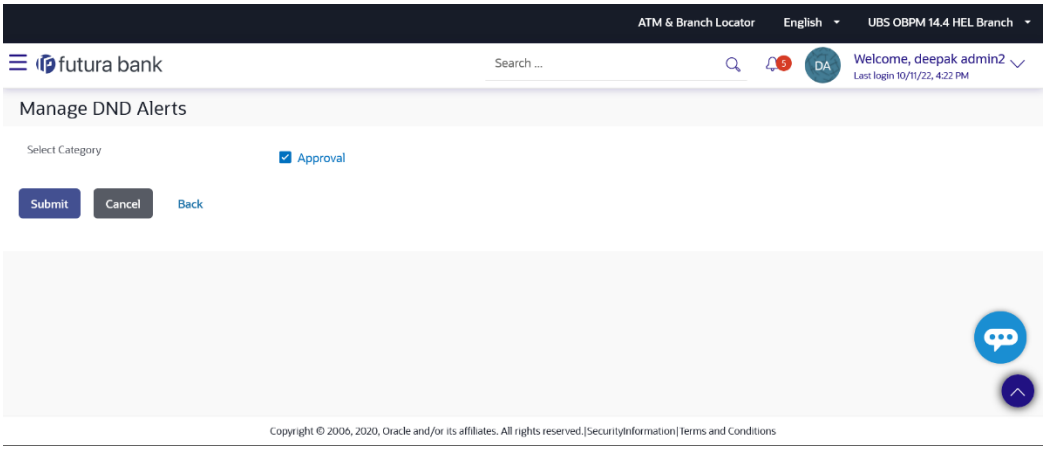
Pre-requisites

- The user must have valid login credentials to access the digital banking platform.

How to reach here:

System/ Bank Administrator Dashboard > Toggle Menu > Menu > Account Settings > Manage DND Alerts

Manage DND Alerts



Field Description

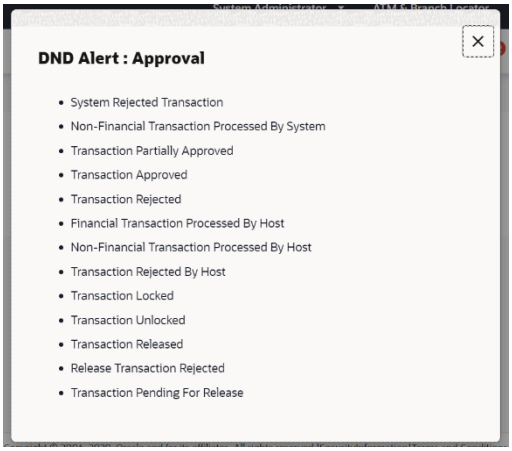
Field Name	Description
Select Category	Select the categories for which DND need to be configured. All the categories configured for DND are listed for selection. Note: Click on category link to view list of all the events for which alerts will not be sent to the user.

To set DND alerts :

2. In the **Select Category** field, select the desired categories for which DND need to be configured.

   b. Click on category link to view list of all the events for which alerts will not be sent to the user.

DND Alerts



3. Click **Submit**.
   A message confirming DND alert set appears.
   OR
   Click **Cancel** to cancel the transaction.
   OR
   Click **Back** to navigate back to the previous screen.

69. Session Timeout

Session timeout represents the event occurring when a user does not perform any action on an application during a configured interval .

The below configurations are provided:

- To configure the inactive screen time. It is a backend configuration where the inactive time after which a warning message will be shown can be configured. This time needs to be lower than the configured active timeout. Note: Default inactive screen time is configured as 10 minutes
- To configure if timeout warning needs to be shown or not. Session timeout warning configuration flag is added on the System Configuration screen

The session timeout feature is available across Oracle Banking Digital Experience product i.e., for Retail User, Corporate User and Administrator screens.

A timeout warning message will be shown when the configured inactive time is reached. The user can view the time remaining for timeout in the warning message. The below actions will be visible to the user on the timeout warning message:

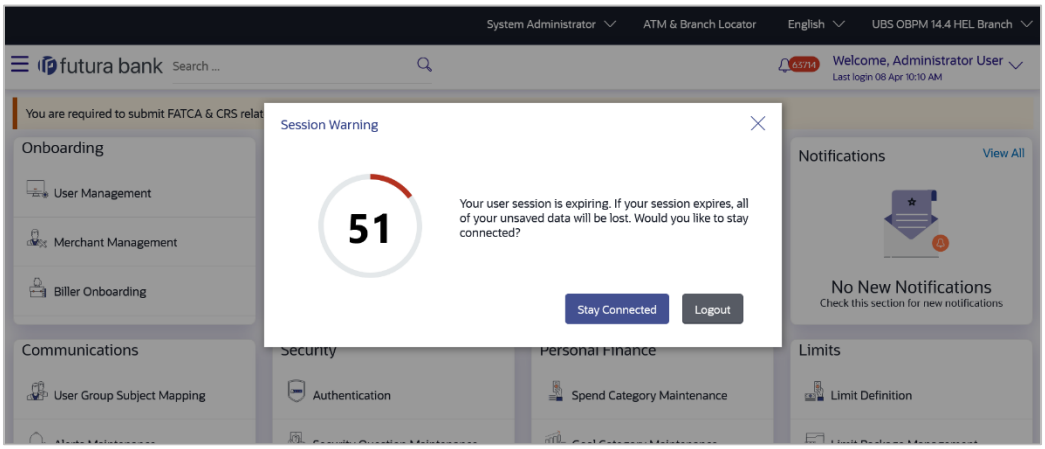
1. Stay Connected
2. Logout

When the user clicks on 'Stay Connected', whichever transaction the user was on will be shown with any pre-filled information previously captured. When the user clicks on ‘Logout’, the user will be logged out of the application. At the end of timeout, the ‘Login’ option will be shown to the user as the session is expired.

Note:
• In case the user clicks on ‘x’ (right hand side top corner on popup), then the popup will close but the timer would continue in the backend. If any action is performed, then timer will reset

• On timeout, if the user clicks on ‘x’ (right hand side top corner on popup) or login button, the login page will appear.

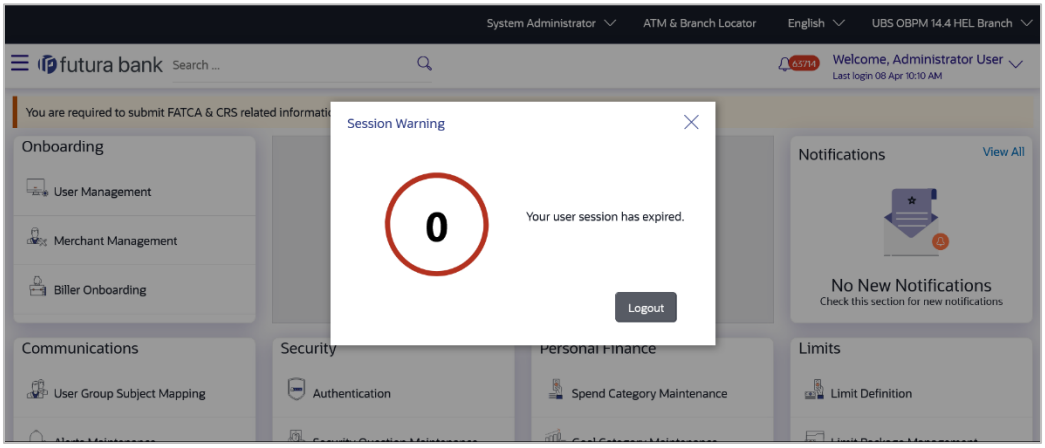
Session Waring – Pre Session Timeout Message



4. Click **Stay Connected** to continue.
   OR
   Click **Logout** to log out of the application.

When the session expires, the **Session Warning** popup appears.

Session Waring- Post Session Timeout Message



1. Click **Login** to re-login to the application.

70. ATM & Branch Locator

Using this option a user can view the address and location of the ATMs and the branches of the Bank available to serve the user in a certain location. The user is provided with the options to search for the bank's ATMs and branches in his vicinity by entering a location. The search results display the list of ATMs / branches name and distance from the user's current location.

This feature enables the user to locate the bank's ATMs/ branches available within a specific radius of his current location. The user can select a Branch / ATM from the search list and on clicking the **View Details** icon; the user will be able to view the address and services provided by the specific ATM/ branch. The additional filter feature is provided to search the ATM/Branch based on their services. In addition the user can view the detailed directions to the ATM/ branch by clicking **Get Directions**, and will also be able to view its location on a map.

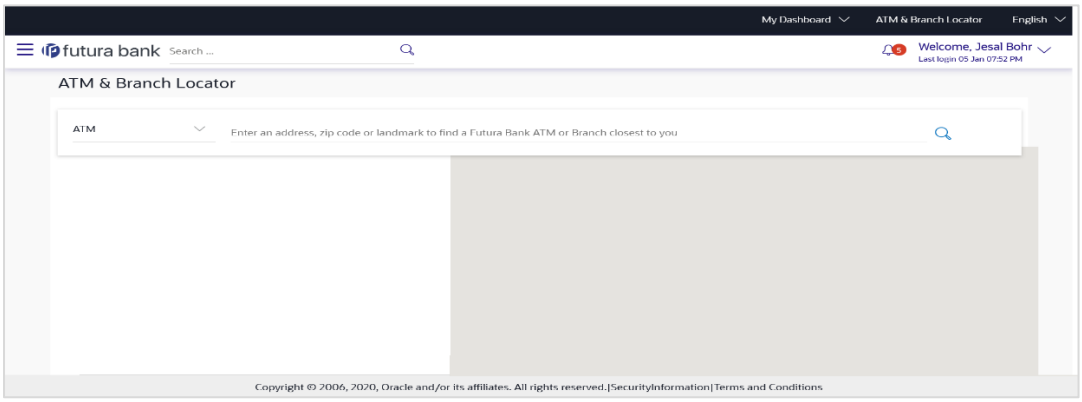
Features supported in the application

- Locate Branches
- Locate ATMs

How to reach here:

OBDX portal landing page> ATM & Branch Locator
OR
Dashboard > Toggle Menu > Menu > ATM & Branch Locator
OR
Dashboard > ATM & Branch Locator

ATM & Branch Locator



Field Description

Field Name	Description
ATM & Branch	Specify whether you want to search for the bank's ATMs or branches. The options are: • ATM • Branch

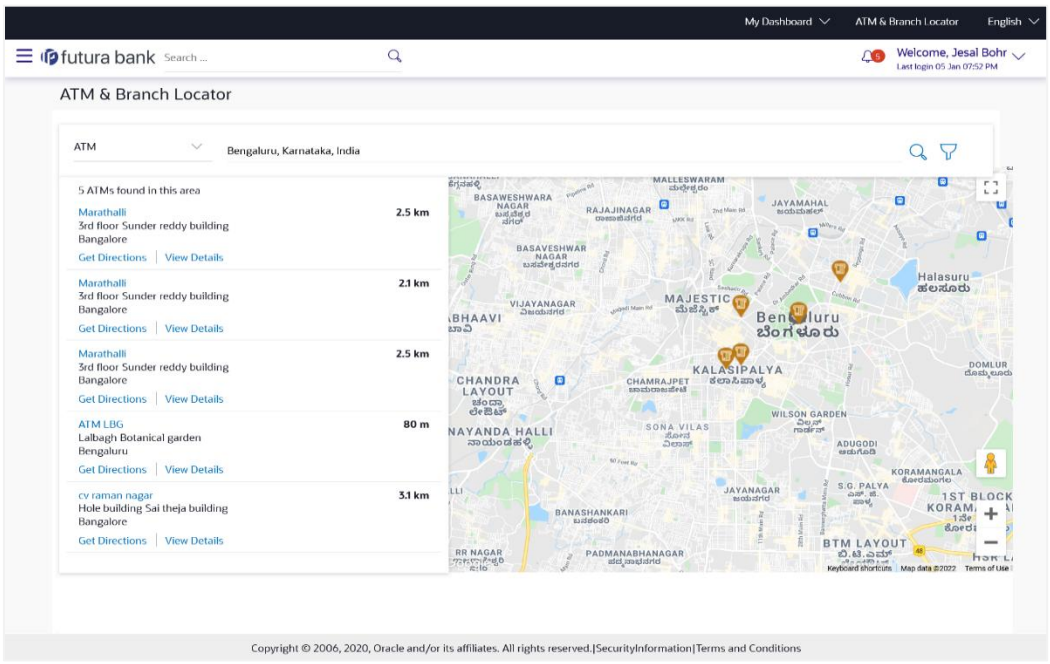
To locate an ATM or Branch

2. Select the desired option and enter the location in which you wish to locate ATMs or Branches:

   c. If you select the **Branch** option, the list of all the branches and their locations appear.

   d. If you select the **ATM** option, the list of all the ATMs and their locations appear.

ATM & Branch Locator - Search



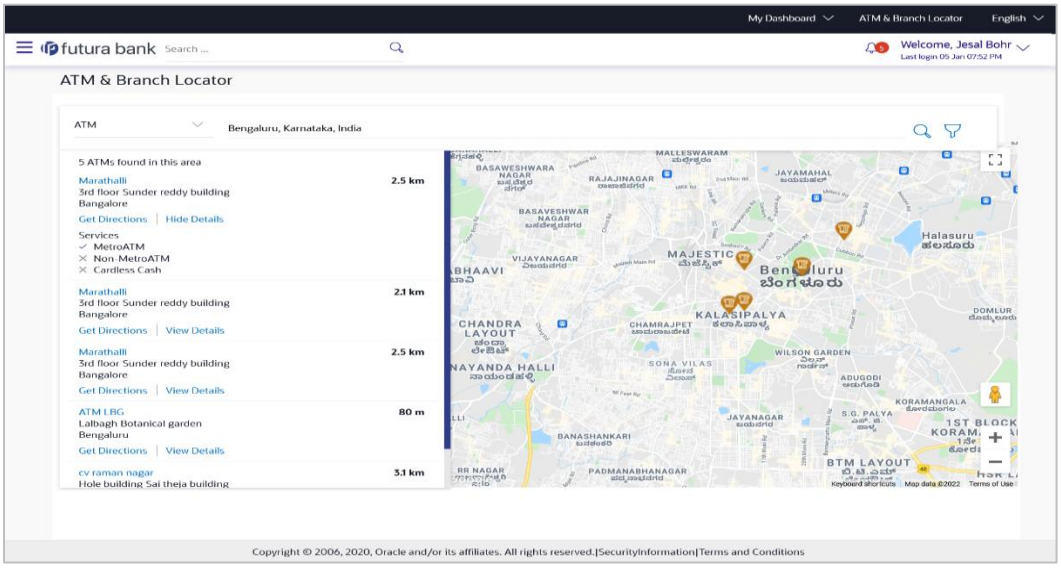
Field Description

Field Name	Description
Location	Key in the address/location/pin-code or city to search for an ATM / Branch.
Number of ATMs/Branches	A statement identifying the number of ATMs/Branches, as the case may be, will be displayed
The following will be displayed per ATM/Branch record:	
Name	The name of the ATM / branch.
Distance	The distance of the ATM / branch from the location entered.
Address	The address of the ATM / branch that you have searched for.

Field Name	Description
Get Directions	Click the link, to view the directions to the branch / ATM from your current location in the map.
View Details	
Clicking this link displays the following details.	
Services	The services offered by the bank's ATM / branch.
Additional Information	Any additional information of the bank's ATM/branch as maintained with the bank will be displayed.

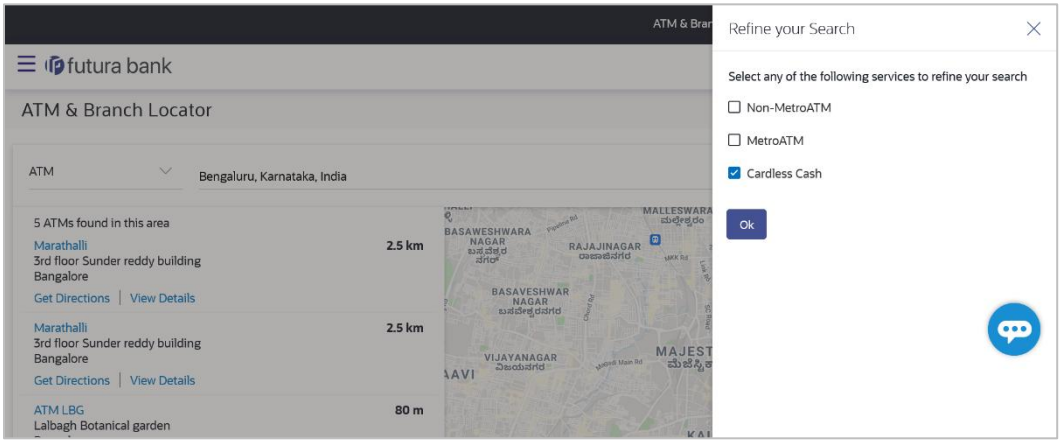
3. In the **Search** box, enter the desired location. The list of ATMs / branches with Name and Distance details appear.
4. Click the icon to view the ATMs/branches in the location entered.
5. Click the View Details link, to view the detailed address, phone number (applicable for a branch), work timings (applicable for a branch) and services provided by the bank branch/ ATM.
6. Click the to filter ATMs or Branches on the basis of services that the ATMs or Branches provide.

ATM & Branch Locator - View Details



7. Click on **Hide Details** to hide the details of the specific ATM/branch.
   OR
   Hover over the ATM/branch marker on the map to view the address of the ATM/branch.
   OR
   Click the to filter ATMs or Branches on the basis of services that the ATMs or Branches provide.

ATM & Branch Locator – Refine your Search

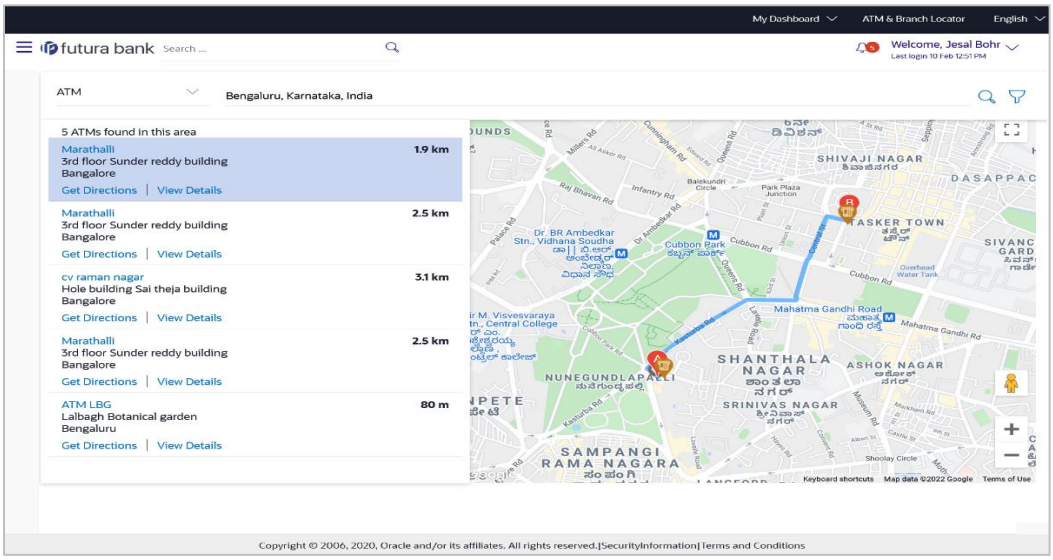


Field Description

Field Name	Description
Service	The list of services provided by the bank in the bank's ATMs or Branches will be listed down with checkboxes available against each. Select any checkbox to filter your search for ATMs or Branches on the basis of service.

8. Select any checkbox to filter your search for ATMs or Branches on the basis of desired service.
9. Click **Ok** to search for ATMs or Branches on the basis of the services selected. The system filters ATMs/Branches on the basis of services selected.

ATM & Branch Locator – Get Directions



10. Hover over the ATM/branch marker on the map to view the address of the ATM/branch.

FAQ

1. **Can I view ATM/ Branches of other cities/ states/ countries?**

   Yes, you can view the ATMs or Branches of the bank located in any city/state or country in the map and also get their details such as address and phone numbers, working hours, services offered, etc.