

Oracle® Banking Microservices Architecture

Party Configurations User Guide



14.7.1.0.0

F84087-01

May 2023

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

F84087-01

Copyright © 2020, 2023, Oracle and/or its affiliates.

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.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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 fail-safe, 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.

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

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	v
Related Documents	v
Conventions	v
Acronyms and Abbreviations	vi
List of Topic	vi
Symbols and Icons	vi
Basic Actions	vi
Screenshot Disclaimer	vii

1 Configurations

1.1	Address Management	1-2
1.2	Credit Rating Agency	1-4
1.2.1	Create Credit Agency	1-5
1.2.2	View Credit Agency	1-6
1.3	Entity Maintenance	1-6
1.4	Host Configuration	1-8
1.5	Location Maintenance	1-9
1.6	Mask Maintenance	1-10
1.7	Organization Maintenance	1-12
1.8	Customer Access Group	1-13
1.9	PII Masking Maintenance	1-15
1.10	Properties Maintenance	1-19
1.11	System Maintenance	1-21
1.12	Service Level Agreements (SLA)	1-23
1.12.1	Setup Service Level Agreements	1-23
1.12.2	OBRH Configurations	1-23
1.12.3	Core Maintenance	1-23
1.12.4	Branch Working Time Setup	1-26
1.13	SLA Calculation	1-26
1.14	SLA Widgets	1-27
1.15	Dynamic Task Allocation	1-28

1.15.1	Setup Dynamic Task Allocation	1-29
1.15.1.1	Plato Configuration	1-29
1.15.1.2	Fact Creation	1-30
1.15.1.3	Rule Creation	1-31
1.15.1.4	Rule Group Creation	1-32
1.15.1.5	Entry in TASK_CONFIG table	1-33
1.15.2	Task Allocation Process	1-34
1.15.3	Postman Collection for Rules APIs	1-34
1.16	Multi-Level Authorization	1-35
1.16.1	Setup Multi-Level Authorization	1-35
1.16.2	Additional Field Configuration	1-39
1.16.3	Upload Source for Common Core (CMC) Party Replication	1-41
1.17	Regional Configuration	1-42

Index

Preface

This topic contains the following subtopics:

- [Audience](#)
- [Related Documents](#)
- [Conventions](#)
- [Acronyms and Abbreviations](#)
- [List of Topic](#)
- [Symbols and Icons](#)
- [Basic Actions](#)
- [Screenshot Disclaimer](#)

Audience

This guide is intended for

1. Implementation team for Day Zero Maintenance of configuration in Oracle Banking Party
2. Bank's Team responsible for Maintenance of configurations in Oracle Banking Party as part of sustenance process

Related Documents

For more information, see these Oracle resources:

- *Getting Started User Guide*
- *Oracle Banking Common Core User Guide*
- *Oracle Banking Security Management System User Guide*

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.
<i>italic</i>	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.

Acronyms and Abbreviations

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

Table 1 Acronyms and Abbreviations

Abbreviation	Description
PII	Personally Identifiable Information

List of Topic

This guide is organized into the following topic:





Table 2 List of Topic

Topic	Description
Configurations	This topic provides an overview of the Configuration Maintenance in Oracle Banking Party and covers the actions to be performed during Configuration Maintenance.

Symbols and Icons

The following are the symbols you are likely to find in this guide:

Table 3 Symbols and Icons

Symbol/Icon	Function
+	Add icon
<Edit>	Edit icon
<Delete>	Delete icon
<Calendar>	Calendar icon
	Close icon
	Expand view
	Maximize
	Minimize

Basic Actions

Most of the screens contain buttons to perform all or few of the basic actions. The following table gives a snapshot of them:

Table 4 Basic Actions

Action	Description
Cancel	On click of Cancel, the system will ask for confirmation and on confirming the task will be closed without saving the data.
Next	On click of Next, the details of the captured will be saved and then system will move to the next screen. If mandatory fields have not been captured, system will display error until the mandatory fields have been captured. If mandatory fields have not been captured, system will display error until the mandatory fields have been captured.
Back	On click of Back, the details of the captured will be saved and then system will move to the previous screen.
Save and Close	On click of Save and Close, the captured details will be saved. If mandatory fields have not been captured, system will display error until the mandatory fields are captured.

Screenshot Disclaimer

Information used in the interface or documents are dummy, it does not exist in real world, and its only for reference purpose.

1

Configurations

Configurations Maintenance is a process to setup and prepare to build application for end-user user. Configurations are commonly done as per the client and end-user requirements.

Prerequisites:

Specify **User ID** and **Password**, and login to **Home** screen. For information on login procedure, refer to the *Getting Started User Guide*.

This topic contains the following subtopics:

- [Address Management](#)
Address management maintenance describes the systematic instructions to initiate and view the address maintenance.
- [Credit Rating Agency](#)
Credit Rating Agency maintenance describes the systematic instruction to initiate and view the credit rating.
- [Entity Maintenance](#)
This topic describes the systematic instructions to initiate and view the Entity maintenance.
- [Host Configuration](#)
Host configuration is to configure the source systems for Retail Party View 360 information.
- [Location Maintenance](#)
This topic describes the systematic instructions to initiate and view the Location maintenance.
- [Mask Maintenance](#)
This topic describes the systematic instructions to initiate and view the Mask maintenance.
- [Organization Maintenance](#)
This topic describes the systematic instructions to initiate and view the Organization maintenance.
- [Customer Access Group](#)
This topic describes the information about the Customer Access Group configurations.
- [PII Masking Maintenance](#)
This topic describes the systematic instructions to initiate and view the PII Masking configurations.
- [Properties Maintenance](#)
Properties maintenance describes the systematic instructions to view and update the key properties.
- [System Maintenance](#)
System maintenance describes the systematic instructions to configure system behavior properties.

- [Service Level Agreements \(SLA\)](#)
This topic describes the information about the Service Level Agreements.
- [SLA Calculation](#)
This topic describes the information about the SLA Calculation.
- [SLA Widgets](#)
This topic describes the information about the SLA Widgets.
- [Dynamic Task Allocation](#)
This topic describes the information about the Dynamic Task Allocation.
- [Multi-Level Authorization](#)
This topic describes the information about the Multi-Level Authorization.
- [Regional Configuration](#)
Regional configuration framework is provided by Plato to enable and configure products within the Oracle Banking Microservices Architecture framework as per regional requirements.

1.1 Address Management

Address management maintenance describes the systematic instructions to initiate and view the address maintenance.

This screen is to enable financial institutions to configure address related requirements.

Using Address Management maintenance, the user can configure:

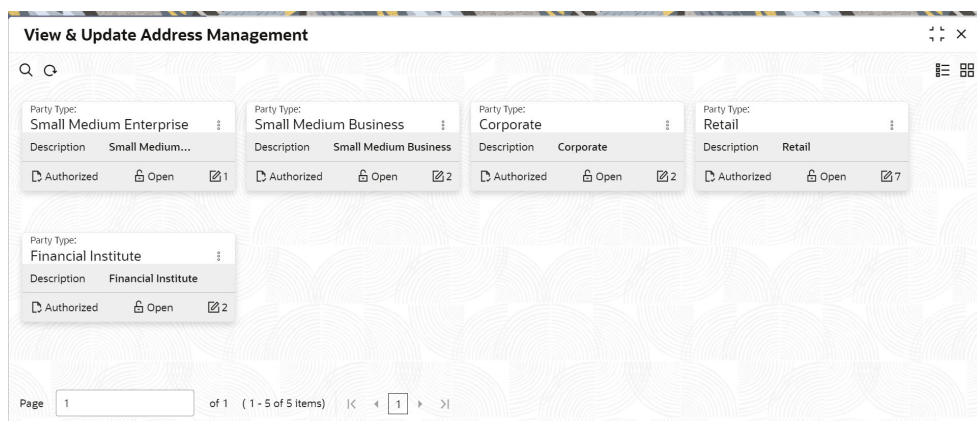
- Mandatory and optional address types
- Minimum address requirement

To initiate Address Management

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Address Management**. Under **Address Management**, click **View & Update Address Management**.

The **View & Update Address Management** screen is displayed.

Figure 1-1 View and Update Address Management



3. Select the required **Party Type**, and click **Unlock** to maintain address management configuration.

The **Create Minimum Address** screen is displayed.

Figure 1-2 Create Minimum Address

4. On the **Create Minimum Address** screen, specify the fields. For more information on fields, refer to the field description table.

Table 1-1 Create Address Management - Field Description


Field	Description
Address Type	<p>Select the address type from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • Permanent Address • Residential Address • Communication Address • Office Address <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;"> <p> Note:</p> <ul style="list-style-type: none"> • This field is mandatory. In case of no configuration for an address type, the same will be optional during onboarding and amendment. • The drop-down values are based on the configuration maintained in the Entity Code Maintenance screen. </div>
Is Mandatory	<p>Enable toggle button if the address type is required to capture during party onboarding and amendment process. For more information, refer to the Table 1-2.</p>

Table 1-1 (Cont.) Create Address Management - Field Description


Field	Description
Minimum Address History (Months)	<p>Provide a value to define what the minimum address history is required to be captured during party onboarding and amendment process.</p> <div style="border-left: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Note:</p> <p>This field accepts only a numeric value without a decimal place.</p> </div>
Action	Click the necessary icon to edit, save, or delete a row.

Table 1-2 Behavior of Current Address Data Segment

Is Mandatory	Minimum Address History	Behavior
Enabled	0 (Zero) Month or No Value	During the party onboarding and amendment, the respective address will be mandatorily captured without any minimum address history validation.
Enabled	Value starting from 1 Month and More	During the party onboarding and amendment, the respective address will be mandatory to be captured with minimum address history validation.
Disabled	0 (Zero) Month or No Value	During the party onboarding and amendment, address capture will be optional.

1.2 Credit Rating Agency

Credit Rating Agency maintenance describes the systematic instruction to initiate and view the credit rating.

This screen is to configure credit rating agencies as required during the Small and Medium Enterprise, Corporate, and Financial Institution Onboarding and Amendment process.

This topic contains the following subtopics:

- [Create Credit Agency](#)
Create Credit Agency maintenance describes the systematic instruction to create the credit rating.
- [View Credit Agency](#)
View Credit Agency maintenance describes the systematic instruction to view the credit rating.

1.2.1 Create Credit Agency

Create Credit Agency maintenance describes the systematic instruction to create the credit rating.

This screen is to configure credit rating agencies as required during Small and Medium Enterprise, Corporate, and Financial Institution Onboarding and Amendment process.

To Create Credit Agency Maintenance

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Credit Rating Agency**. Under **Credit Rating Agency**, click **Create Credit Agency**.

The **Create Credit Agency** screen is displayed.

Figure 1-3 Create Credit Agency

3. On the **Create Rating Agency** screen, specify the fields. For more information on fields, refer to the field description table.

Table 1-3 Credit Rating Agency - Field Description

Field	Description
Agency code	Specify the agency code.
Agency Description	Specify the description of the agency code.
Agency Type	Select type of the agency from the drop-down list. The available values are: <ul style="list-style-type: none"> • Internal • External
Rating Code	Specify the rating code of the credit agency.
Rating Description	Specify the description of the rating code.
Actions	Click the necessary icon to perform the below actions: <ul style="list-style-type: none"> • Edit • Save • Delete

4. Click **Save**.

1.2.2 View Credit Agency

View Credit Agency maintenance describes the systematic instruction to view the credit rating.

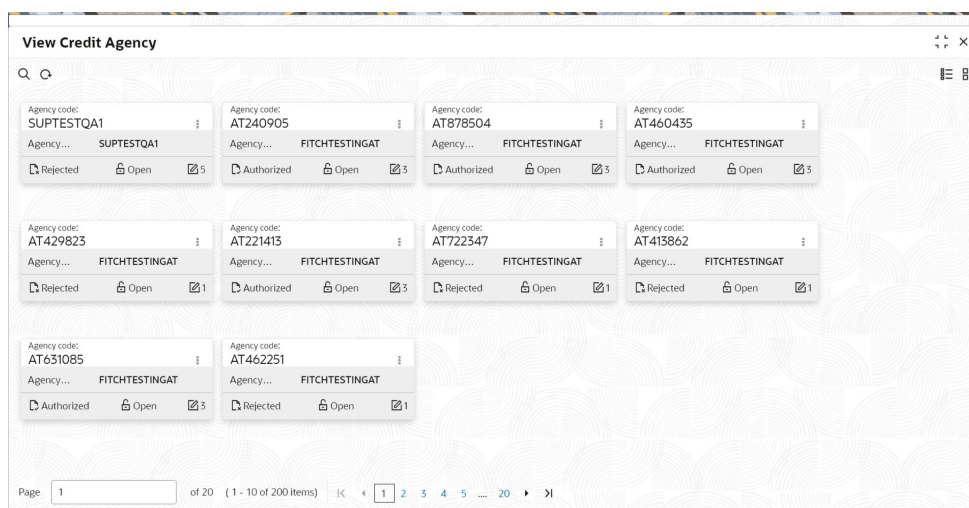
This screen is to configure credit rating agencies as required during Small and Medium Enterprise, Corporate, and Financial Institution Onboarding and Amendment process.

To View Credit Agency Maintenance

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Credit Rating Agency**. Under **Credit Rating Agency**, click **View Credit Agency**.

The **View Credit Agency** screen is displayed.

Figure 1-4 View Credit Agency



You can view a summary of the configured records for the credit agency details on this screen.

1.3 Entity Maintenance

This topic describes the systematic instructions to initiate and view the Entity maintenance.

Entity Maintenance enables the user to easily configure and maintain entity codes used in system from UI screen rather than inserting it in Database.

Using Entity Maintenance, the user will be able to

- Add, Delete and Modify entity codes
- Add, Delete, Modify sub-entity codes for each of the entity codes

Initiate Entity Maintenance

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Entity**. Under **Entity**, click **Create Entity**.
The **Create Entity** screen displays.

Figure 1-5 Create Entity

3. On **Create Entity** screen, specify the following attributes.
For more information on fields, refer to the field description table.

Table 1-4 Create Entity - Field Description

Field	Description
Entity Code	Specify the entity code to be define with the list of drop-down values.
Entity Description	Specify the description of the entity code.
Language	Language of the entity code.
Sub Entity Code	Specify the Sub Entity Code for the selected Entity Code.
Sub Entity Description	Specify the description of Sub Entity Code.
Retail	Enable toggle button if the sub-entity code is applicable for retails party.
SMB	Enable toggle button if the sub-entity code is applicable for SMB party.
Corporate	Enable toggle button if the sub-entity code is applicable for corporate party.
SME	Enable toggle button if the sub-entity code is applicable for SME party.
FI	Enable toggle button if the sub-entity code is applicable for financial institution party.

4. Click + button to add Sub-entities for Entity Code.
5. Click **Save**.

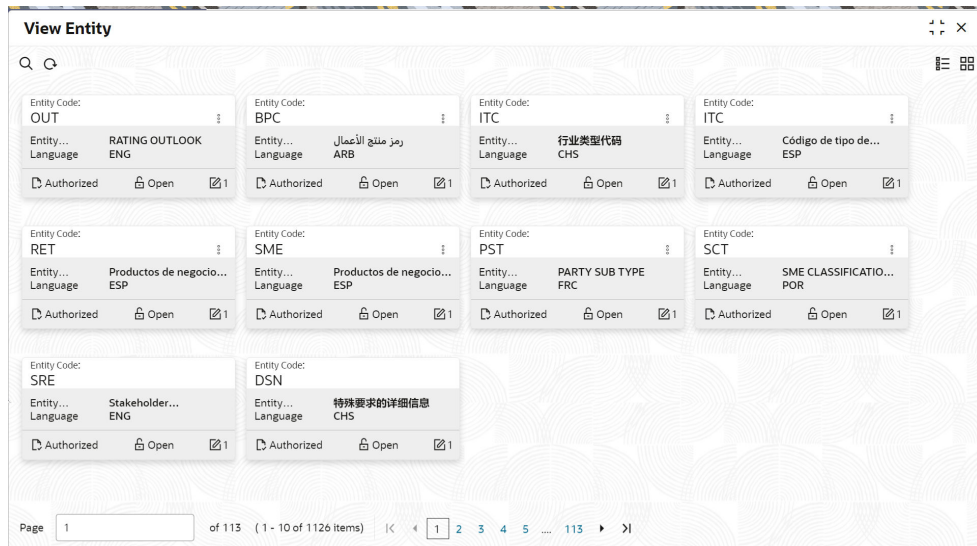
View Entity Maintenance

Once the record is authorized by the checker, the user can view the Entity Maintenance.

6. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.

- Under **Maintenance**, click **Entity**. Under **Entity**, click **View Entity**.
The **View Entity** screen displays.

Figure 1-6 View Entity



1.4 Host Configuration

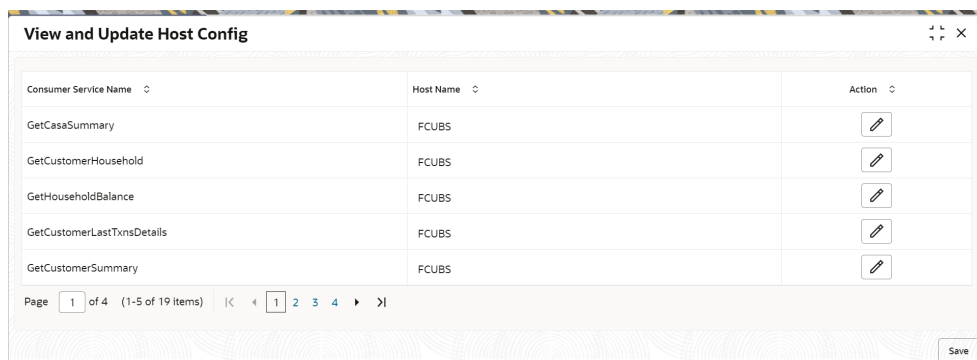
Host configuration is to configure the source systems for Retail Party View 360 information.

To initiate Host Configuration

- On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
- Under **Maintenance**, click **Host Config**. Under **Host Config**, click **View and Update Host Config**.

The **View and Update Host Config** screen is displayed.

Figure 1-7 View and Update Host Config



- On the **View and Update Host Config** screen, specify the fields. For more information on fields, refer to the field description table.

Table 1-5 Host Configuration - Field Description

Field	Description
Consumer Service Name	Displays the consumer service name.
Host Name	Displays the host name.
Action	Click the necessary icon to edit, save, or delete a row.

4. Click **Save**.

1.5 Location Maintenance

This topic describes the systematic instructions to initiate and view the Location maintenance.

Location Maintenance enables the user to add, delete and modify Location Codes. Location Codes can be captured during party onboarding and amendment process to identify precise location of the customer. Location codes can be specific definition of locations within a specified area by the financial institutions.

Initiate Location Maintenance

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Location**. Under **Location**, click **Create Location**.

The **Create Location** screen displays.

Figure 1-8 Create Location

3. On **Create Location** screen, specify the following attributes.
For more information on fields, refer to the field description table.

Table 1-6 Create Location - Field Description

Field	Description
Location Code	Specify the specific location code, which can be selected during Party onboarding and amendment process.
Location Description	Specify the description of the location code.

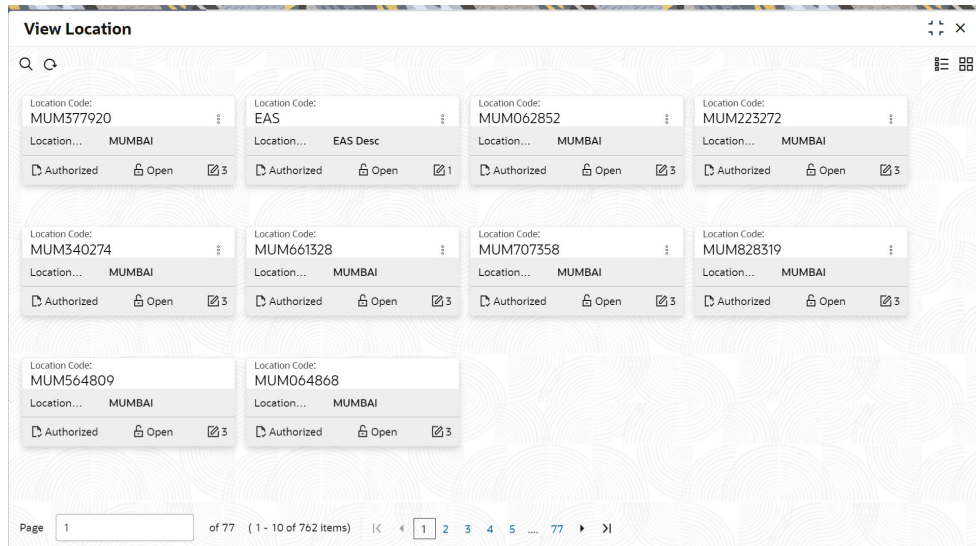
4. Click **Save** to save the location code.

View Location Maintenance

Once the record is authorized by the checker, the user can view the Location Maintenance.

5. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
6. Under **Maintenance**, click **Location**. Under **Location**, click **View Location**. The **View Location** screen displays.

Figure 1-9 View Location



1.6 Mask Maintenance

This topic describes the systematic instructions to initiate and view the Mask maintenance.

Mask Maintenance enables the user to create a mask for defining the Party Id format.

Note:

If no Mask Maintenance is configured, the default party id will be generated as “YYJJSSSS” wherein,

- YY** – Current Year
- JJJ** – Julian Date of current year
- SSSS** – Sequence Number

Initiate Mask Code Maintenance

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Mask**. Under **Mask**, click **Create Mask**. The **Create Mask** screen displays.

Figure 1-10 Create Mask

3. On **Create Mask** screen, specify the following attributes.
For more information on fields, refer to the field description table.

Table 1-7 Create Mask - Field Description

Field	Description
Mask Code	Select the mask type as Party Id from the dropdown list.
Component	Displays the attribute name added from the list.
Mask	Specify the total length of the mask, which is the sum of length of all the attributes in the mask cannot exceed 36 characters. If no mask is defined, a default mask – PTYddddssss is applicable which includes: <ol style="list-style-type: none"> a. Prefix with values PTY b. Julian Date (dddd) c. Sequence Number (ssss) of length 4 characters
Delete	Click this icon to delete the added parameter.

4. Click **Add** button to add the parameters for the Party Id Mask.
5. Add the following attributes:
 - a. Prefix Code (**PTY**) – a prefix that can be attached to the party id. This attribute is optional and editable.
 - b. Branch Code (**bbb**) – The branch code of the user logged in branch. This attribute is optional and non-editable.
 - c. Julian Date (**dddd**) – The Julian date in **YYDDD** format on which the party is being onboarded. This attribute is optional and non-editable.
 - d. Sequence Number (**ssss**) – A sequence number that can be appended to the party id. The system will generate the sequence number based on the length defined in the mask. This attribute is mandatory and editable.
6. Click **Save** to save the party id mask.

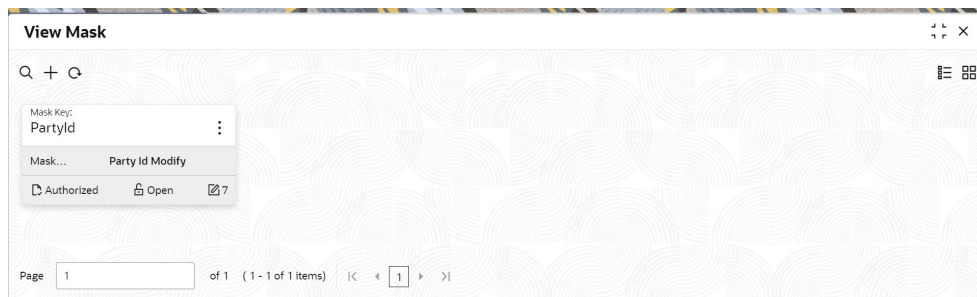
View Mask Maintenance

Once the record is authorized by the checker, the user can view the Entity Maintenance.

7. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
8. Under **Maintenance**, click **Mask Management**. Under **Mask Management**, click **View Mask**.

The **View Mask** screen displays.

Figure 1-11 View Mask



1.7 Organization Maintenance

This topic describes the systematic instructions to initiate and view the Organization maintenance.

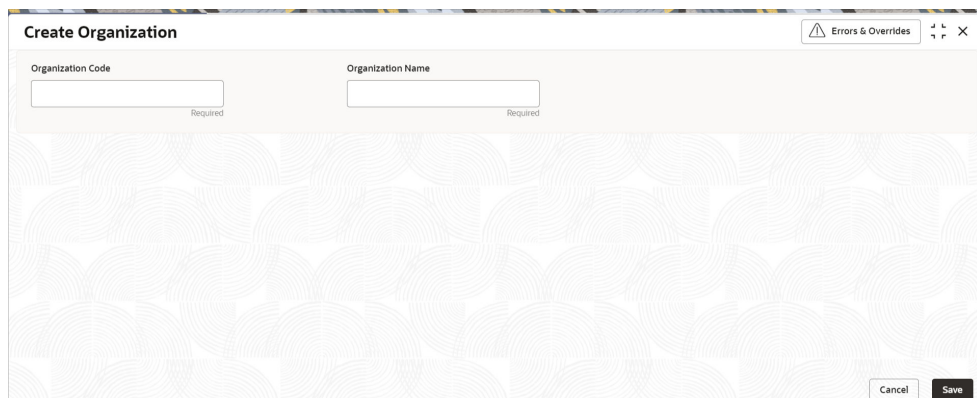
Organization Maintenance functionality allows user to add, delete and modify Organizations Codes and respective description of the Organization.

Initiate Organization Maintenance

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Organization**. Under **Organization**, click **Create Organization**.

The **Create Organization** screen displays.

Figure 1-12 Create Organization



3. On **Create Organization** screen, specify the following attributes.
For more information on fields, refer to the field description table.

Table 1-8 Create Organization - Field Description

Field	Description
Organization Code	Specify the specific Organization code, which can be selected during Party onboarding and amendment process.
Organization Description	Specify the name of the organization.

- Click **Save** to save the Organization code.

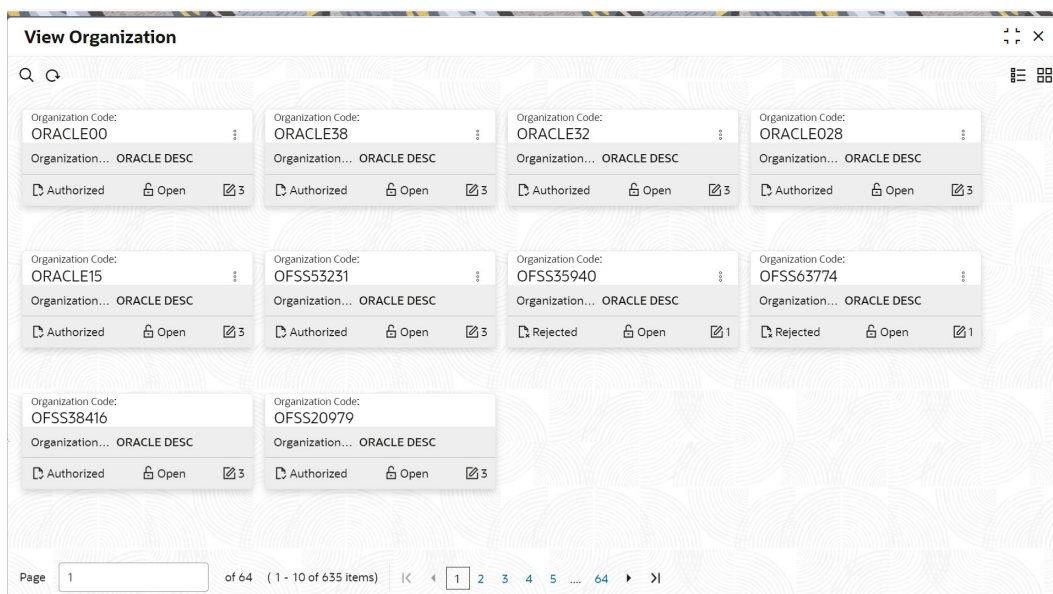
View Organization Maintenance

Once the record is authorized by the checker, the user can view the Entity Maintenance.

- On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
- Under **Maintenance**, click **Organization**. Under **Organization**, click **View Organization**.

The **View Organization** screen displays.

Figure 1-13 View Organization



Note:

A records can be rejected by the authorizer for certain reasons. In such cases, the maintenance will be available to maker for updates and subsequent approval by the authorizer. For more information, refer to Getting Started User Guide.

1.8 Customer Access Group

This topic describes the information about the Customer Access Group configurations.

Customer access group functionality is part of privacy by design requirements. The customer access group will restrict unauthorized access by the users to details of customers within specific customer access groups such as High Net Worth, Sensitive etc.

Customer Access Group Configuration:

Step 1 – Create Customer Access Group (Core Maintenance)

Step 2 – Map Customer Access Group/s to User/s (SMS User Maintenance)

During Party Onboarding and Amendment process, based on the configuration, customer access group can be assigned updated by users.

Customer Access Group is applicable for all customer types – Retail, Small and Medium Business (SMB), Small and Medium Enterprise (SME), Corporate, Financial Institutions (FI).

Example of Customer Access Group:

- Access Groups: AccessGroup_1, AccessGroup_2,
- User: USER1, USER2
- Customers: CUST11, CUST12, CUST13, CUST21, CUST22, CUST23, CUST31, CUST32 & CUST33

Mapping of User and Access Group Restriction and Customer belongs to Access Group as follows:

Table 1-9 Access Group Mapping

USER1	USER2	USER3 & USER4
AccessGroup_1	AccessGroup_2 AccessGroup_3	AccessGroup_3
AccessGroup_1	AccessGroup_2	AccessGroup_3
CUST11 CUST12 CUST13	CUST21 CUST22 CUST23	CUST31 CUST32 CUST33

- USER1 will be able to access customer belonging to AccessGroup_1 only. User will not be able to query CUST21, since CUST21 belongs to AccessGroup_2 which is not allowed for user USER1.
- USER2 will be able to access customer belonging to AccessGroup_2 and AccessGroup_3. User will not be able to access CUST12 belongs to AccessGroup_1 which is not allowed for this user.
- USER3 & USER4 both will be able to access customer belonging to AccessGroup_3 only. User will not be able to access Cust11 or Cust21, belongs to AccessGroup_1 & AccessGroup_2 which is not allowed for this user.



Note:

The customer access group is applicable for stakeholders also. A user will not be able to access details of a stakeholder linked to a party, if user does not have access to customer access group of the linked stakeholder.

For more details, refer to **Oracle Banking Common Core User Guide** and **Oracle Banking Security Management System User Guide**.

1.9 PII Masking Maintenance

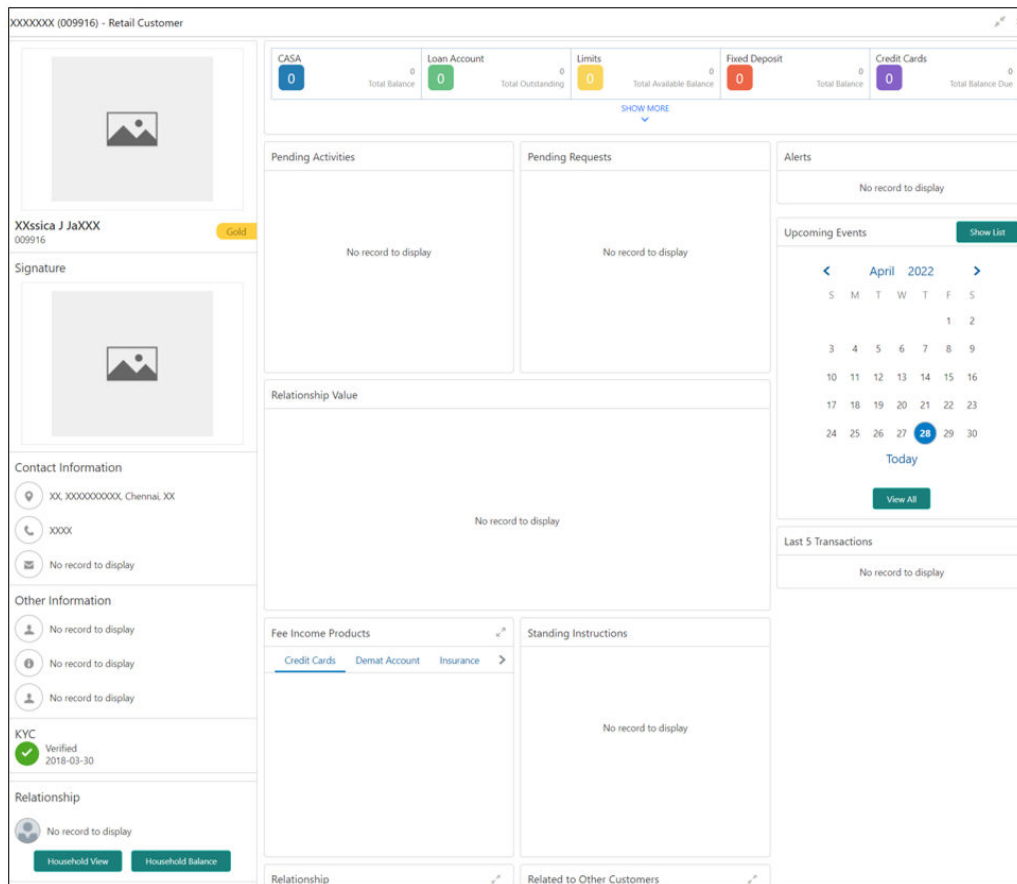
This topic describes the systematic instructions to initiate and view the PII Masking configurations.

Personally Identifiable Information (PII) Masking requirements is part of privacy by design requirements. PII functionality is to restrict unauthorized access by the users to personal information of customer by masking the PII information.

PII Information masking will be as follows

- **PII access is enabled for the user** – PII information will be visible to the user.
- **PII access is disabled for the user** – PII information will be visible as masked information as per defined masks.

Figure 1-14 Sample Masked Information



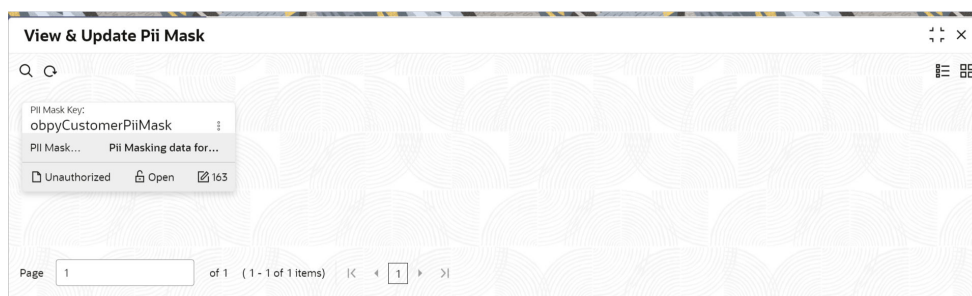
Refer to **Oracle Banking Security Management System User Guide** for more details on enabling and disabling PII access for the user.

Initiate PII Mask Management Configuration

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **PII Mask**. Under **PII Mask**, click **View and Update PII Mask**.

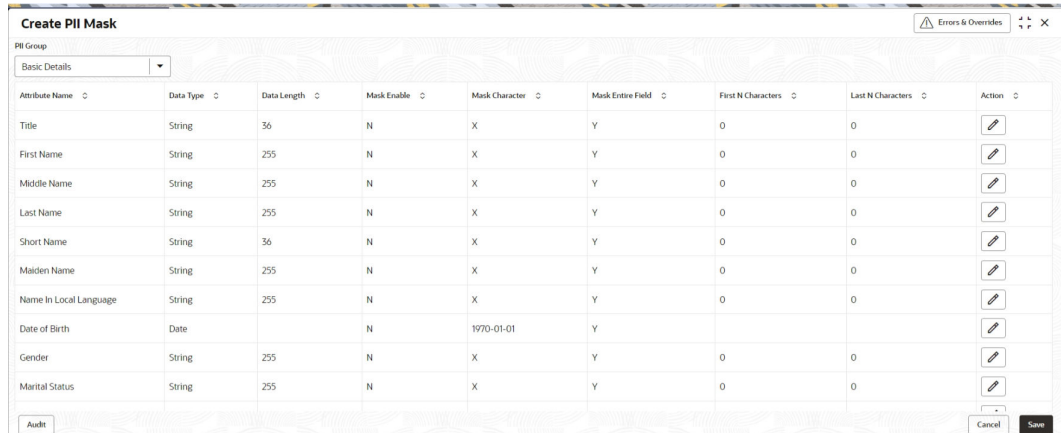
The **View and Update PII Mask** screen displays.

Figure 1-15 View and Update PII Mask



3. Click **Unlock**.
The **Create PII Mask** screen displays.

Figure 1-16 Create PII Mask



4. On **Create PII Mask** screen, select **PII Group**.
For more information on fields, refer to the field description table.

Table 1-10 Create PII Mask - Field Description

Field	Description
PII Group	<p>Select the Logical grouping of PII Fields in the dropdown list. The available values are</p> <ul style="list-style-type: none"> • Basic Details • Address and Contact • ISO Contact • KYC Check • Signature • Address and Contact Host

The List of PII fields will be available in table structure as per selected **PII Group**.

5. Click **Action** button for configuring Mask for each individual PII field.
The **Edit PII Masking** screen displays.

Figure 1-17 Edit PII Masking

- On the **Edit PII Masking** screen, specify the required details in the respective fields.

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

Table 1-11 Edit PII Mask - Field Description

Field	Description
Attribute Name	Displays the attribute name based on the selected PII field.
Data Type	Displays the PII field data type (such as String, Date etc.) based on selected attribute.
Data Length	Displays the PII field length based on selected attribute.
Mask Enable	Select the toggle to identify whether the masking is enabled or disabled for the field. If Mask Enable toggle is ON, the field will be displayed as masked to unauthorized users. If Mask Enable toggle is set as OFF, the field will display without masking to all users.
Mask Characters	Displays the masking character to display, if masking is enabled for PII field.
Mask Entire Field	Select the toggle to identify whether the complete field is masked or not.
First N Character	Specify the number of characters masked from the first character of the field.
Last N Character	Specify the number of characters masked from last character of the field.

 **Note:**

If the **First N Character** and **Last N Character** are overlapping, then the entire field will be masked.

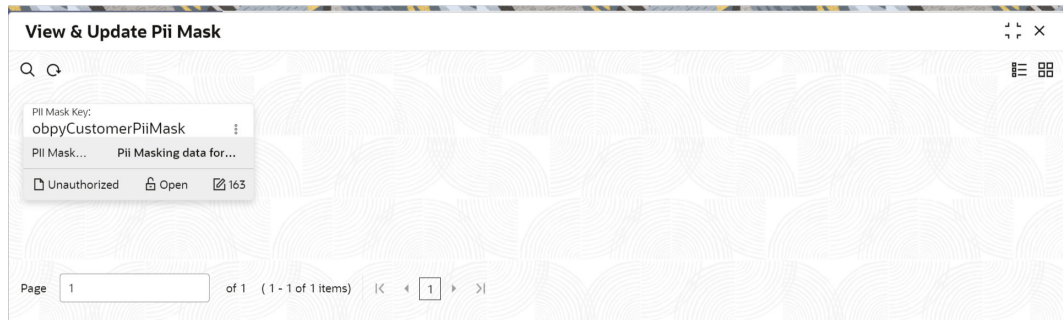
- Click **Save** after completing the masking configuration for all required PII fields.

View PII Mask Management Configuration

Once the record is authorized by the checker, the user can view the PII Mask Management Configuration.

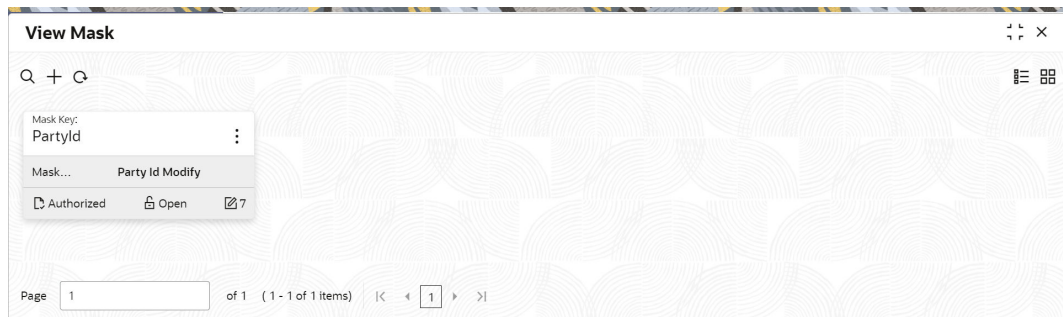
8. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
9. Under **Maintenance**, click **PII Mask**. Under **PII Mask**, click **View and Update PII Mask**.
The **View and Update PII Mask** screen displays.

Figure 1-18 View and Update PII Mask



10. Click **View** to view the defined PII masking.
The **View PII Mask** screen displays.

Figure 1-19 View PII Mask



1.10 Properties Maintenance

Properties maintenance describes the systematic instructions to view and update the key properties.

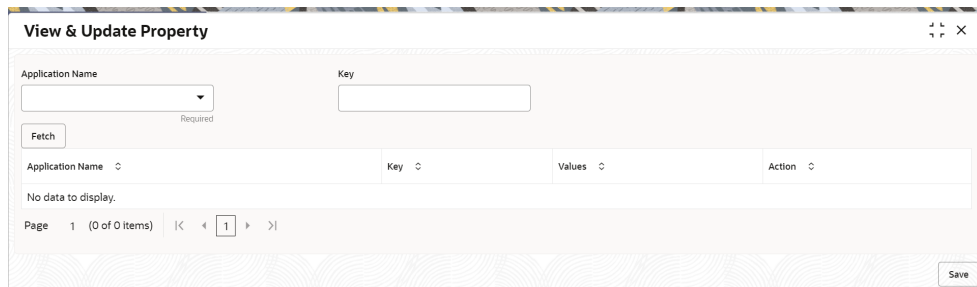
This screen is used to configure the key properties for Oracle Banking Party.

To initiate Host Configuration

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Properties Maintenance**. Under **Properties Maintenance**, click **View & Update Property**.

The **View & Update Property** screen is displayed.

Figure 1-20 View and Update Property



3. On the **View and Update Property** screen, specify the details. For more information on fields, refer to the field description table.

Table 1-12 View and Update Property - Field Description

Field	Description
Application Name	Select the application name from the drop-down list.
Key	Specify the key.
Application Name	Displays the selected application name.
Key	Displays the key of the application.
Values	Displays the value of the application.
Action	Click the necessary icon to edit or save a row.

4. Click **Save**.

The below table provides details of key properties, which can be configured using properties maintenance.

Table 1-13 OBPY Properties Maintenance

ID	Application	Key	Description	Sample Value
7	obpy-party-handoff-services	KYC_FCUBS_SOAP_URL	SOAP API url of FCUBS	http://whf00alo:7348/FCUBSSTService/FCUBSSTService?WSDL
12	obpy-party-services	STP_FLAG	Straight through processing of Retail Party Onboarding	TRUE
13	obpy-party-kyc-services	BANK_MANDATORY_KYCS	Mandatory KYC required. More than one KYC type can be inserted as Pipe () separated	IDVR ADVR
14	obpy-party-kyc-services	BANK_KYC_VALID_IN_MONTHS	KYC validation period	24
1	obpy-party-services	REOB_ADDITIONAL_FIELDS_UIKEY	Unique identification reference key of screens for user defined fields. UIKEY of more than one screen can be inserted as Pipe () separated	fsgbu-ob-cmn-ds-additional-fields@OBPY_REOB_BASIC_ENRH fsgbu-ob-cmn-ds-additional-fields@OBPY_REOB_ENRH

Table 1-13 (Cont.) OBPY Properties Maintenance

ID	Application	Key	Description	Sample Value
2	obpy-party-services	SYNC_REQUIRED	Boolean value to determine if party information refresh is required from FCUBS to OBPY	TRUE
15	obpy-party-handoff-services	CMC_REPLICATION_REQUIRE	Boolean value to determine if replication of party information is required to OBMA Common Core (CMC)	TRUE
16	obpy-party-handoff-services	REOB_ADDITIONAL_FIELDS_UIKEY	Unique identification reference key of screens for user defined fields. UIKEY of more than one screen can be inserted as Pipe () separated	fsgbu-ob-cmn-ds-additional-fields@OBPY_REOB_BASIC_ENRH fsgbu-ob-cmn-ds-additional-fields@OBPY_REOB_ENRH
25	obpy-party-handoff-services	HOST_HANDOFF_REQUIRED	Boolean value to determine if party information required to be handed off to FCUBS from OBPY	TRUE
31	obpy-party-services	MINOR_AGE_CRITERIA	Age criteria for Minor Customer	18
27	obpy-party-services	PII_MASKING_PARTY_TYPES	Type of Parties to be considered for PII masking	I S
28	obpy-party-services	BANK_MANDATORY_KYCS	Mandatory KYC required. More than one KYC type can be inserted as Pipe () separated	IDVR ADV

1.11 System Maintenance

System maintenance describes the systematic instructions to configure system behavior properties.

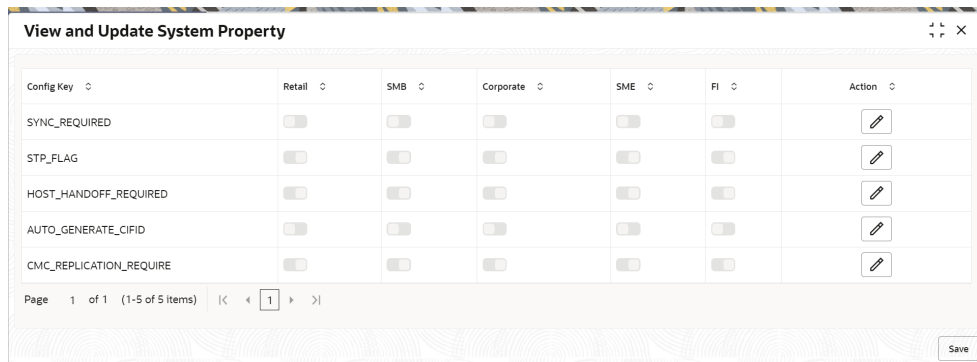
This screen is to configure system behavior properties for different party type such as handoff to host required.

To initiate System Maintenance

1. On **Home** screen, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **System Maintenance**. Under **System Maintenance**, click **View and Update System Property**.

The **View and Update System Property** screen is displayed.

Figure 1-21 View and Update System Property



3. On the **View and Update System Property** screen, specify the fields. For more information on fields, refer to the field description table.

Table 1-14 View and Update System Property - Field Description

Field	Description
Config Key	Displays the configuration key.
Retail	Enable toggle button if required for the config key.
SMB	Enable toggle button if required for the config key.
Corporate	Enable toggle button if required for the config key.
SME	Enable toggle button if required for the config key.
FI	Enable toggle button if required for the config key.
Action	Click the necessary icon to edit or save a row.

The system property for the config key can be updated using system maintenance for different party types. For more information on the configuration key, refer to the [Table 1-15](#)

Table 1-15 Config Key Description

Config Key	Description
SYNC_REQUIRED	Configuration to enable or disable party information sync with host system for different party types.
STP_FLAG	Configuration to enable or disable straight through processing for different party types.
HOST_HANDOFF_REQUIRE	Configuration to enable and disable host handoff for different party types.
AUTO_GENERATE_CIFID	Configuration to enable and disable party id generation for different party types.
CMC_REPLICATION_REQUIRED	Configuration to enable and disable party information replication to common core external customer for different party types.

4. Click **Save**.

1.12 Service Level Agreements (SLA)

This topic describes the information about the Service Level Agreements.

Service Level Agreements (SLA) is an important aspect of banking services from the customer and internal bank policy perspectives. Bank would like to maintain and adhere to SLA's during various operations and stages within banking processes. The SLA functionality is designed to provide the expected completion times for all the tasks/processes configured for SLA.

Service Level Agreement is provided as Plato framework.

- [Setup Service Level Agreements](#)
This topic describes the information to setup Service Level Agreements.
- [OBRH Configurations](#)
This topic describes the systematic instructions to configure the OBRH for Service Level Agreements.
- [Core Maintenance](#)
This topic describes the systematic instructions to create and view the Core maintenance for Service Level Agreements.
- [Branch Working Time Setup](#)
This topic describes the information about the Branch Working Time Setup.

1.12.1 Setup Service Level Agreements

This topic describes the information to setup Service Level Agreements.

1.12.2 OBRH Configurations

This topic describes the systematic instructions to configure the OBRH for Service Level Agreements.

1. Download and import <SLA_API_Consumer> json in Service Consumers to set up the OBRH service for cmc-sla-service to fetch business product codes for a given product code.
2. Set up service provider for OBPY with default implementation as follows.
3. In **Consumer Services**, add the following routing.
4. A parameter needs to be maintained in server start parameters for enabling SLA functionality: -Dplato.orchestrator.enableSLA=true. Same parameter also needs to be checked in PROPERTIES table in PLATO schema.

1.12.3 Core Maintenance

This topic describes the systematic instructions to create and view the Core maintenance for Service Level Agreements.

Create SLA in Core Maintenance

1. On **Home** screen, click **Core Maintenance**. Under **Core Maintenance**, click **SLA Maintenance**.
2. Under **SLA Maintenance**, click **Create SLA**.

The **Create SLA** screen displays.

Figure 1-22 Create SLA

3. On **Create SLA** screen, specify the following attributes.
For more information on fields, refer to the field description table.

Table 1-16 Create SLA - Field Description

Field	Description
Product/Application Code	Specify the Product or Application Code as "OBPY".
Product/Application Name	Displays the name of the Product/Application.
Business Process Code	Select the Business Process Code for which the SLA maintenance needs to be maintained.
Business Process Name	Displays the Business Process name pertaining to the Business Process code selected.
Branch Code	Select the branch code for which SLA maintenance needs to be maintained. User can also select "All" as a value which will enable the SLA to be applicable for all branches in the bank.
Branch Name	Displays the branch name pertaining to the branch code selected.
Branch Time	Displays the branch working hours as populated.
Version	Displays the version as defaulted on creating/updating the screen.
Hold Time	Select the checkbox if the hold time is to be considered for SLA calculation.
Branch Holidays	Select the checkbox if the branch holidays is to be considered for SLA calculation.
Currency Holidays	Select the checkbox if the currency holidays is to be considered for SLA calculation.
Customer Clarification	Select the checkbox if the Customer Clarification items is t to be considered for SLA calculation,
Off-Branch Time Transactions	Select the checkbox if the SLA should be calculated after branch hours.

4. To calculate the **SLA Setup**, specify the following attributes.

Table 1-17 SLA Setup - Field Description

Field	Description
Stage Name	Displays the various stages available for the process on selection of the process code.
Stage ID	Displays the stage ID based on the stage name.
Parallel Stage	Displays the parallel stage details.
Time In	Select the time in dropdown values as Mins or Days-Hr-Mins . If Days-Hr-Mins is selected, the system will display a pop-up UI for input of the Stage SLA in Days/Hours/Minutes combination. The system will convert into minutes and display in the respective field. If Mins is selected, the user can directly input the SLA in Minutes.
Low Priority - Offline	Specify the SLA time for Low Priority Offline Applications.
Low Priority - Online	Specify the SLA time for Low Priority Online Applications. The system validates that the time in minutes is not more than the value input for offline.
Medium Priority - Offline	Specify the SLA time for Medium Priority Offline Applications. The system validates that the time in minutes is not more than value for Low Priority.
Medium Priority - Online	Specify the SLA time for Medium Priority Online Applications. The system validates that the time in minutes is not more than value input for offline and Low Priority.
High Priority - Offline	Specify the SLA time for High Priority Offline Applications. The system validates that the time in minutes is not more than value for Medium Priority.
High Priority - Online	Specify the SLA time for High Priority Online Applications. The system validates that the time in minutes is not more than value input for offline and Medium Priority.
Breach SLA Time	Specify the SLA Breach Alert time in minutes for the stage. This indicates the minutes before which a user needs to be alerted for likely SLA breach for the stage. This is the same for all the different priority combinations for a stage irrespective of the individual SLA times.
SLA Required	Select the toggle to indicate whether SLA calculation is required for this stage. By Default, the toggle should be set to Yes. User can change the value to No. If the toggle is changed to No, the user input should be disabled and the SLA values for the stage should be blank.
Total SLA	Displays the value based on the sum of SLA stages.
SLA Near Breach Alert Time (in Minutes)	Specify the minutes before which an impending SLA breach is to be notified to the user. The system validates that this is not more than the SLA in minutes.

5. Click **Calculate** to create the SLA's and calculate the overall SLA for the workflow and populate the total SLA's.
6. Click **Save** to save the SLA details.

View SLA in Core Maintenance

Once the record is authorized by the checker, the user can view the Entity Maintenance.

7. On **Home** screen, click **Core Maintenance**. Under **Core Maintenance**, click **SLA Maintenance**.
8. Under **SLA Maintenance**, click **View SLA**.

1.12.4 Branch Working Time Setup

This topic describes the information about the Branch Working Time Setup.

For Branch Working Time setup, add entries into CMC_TM_BRN_WORKHOURS_MASTER and CMC_TM_BRN_WORKHOURS_DET in CMCORE schema tables for SLA calculation as follows:

Figure 1-23 CMC_TM_BRN_WORKHOURS_MASTER

ID	BRANCH_CODE	RECORD_STAT	AUTH_STAT	ONCE_AUTH	MAKER_ID	MAKER_DT_STAMP	CHECKER...	CHECKER_DT_STAMP	MOD_NO	
1	OBPY_1	000	0	A	Y	MURAL11	22-MAR-19	MURAL11	22-MAR-19	1

Figure 1-24 CMC_TM_BRN_WORKHOURS_DET

ID	BRN_WORKHOURS_MASTER_ID	WEEKDAY	WF_SEQ	START_TIME	END_TIME	WRI_HOURS	IS_OPEN	IS_24HW
1	BRN_WORKHOURS_DET_1	OBPY_1	MON	1 01-JUN-22 09.00.00.362000000	AM 02-JUN-22 07.00.00.016000000	PM 8 Y	N	
2	BRN_WORKHOURS_DET_2	OBPY_1	TUE	2 01-JUN-22 09.00.00.362000000	AM 02-JUN-22 07.00.00.016000000	PM 8 Y	N	
3	BRN_WORKHOURS_DET_3	OBPY_1	WED	3 01-JUN-22 09.00.00.362000000	AM 02-JUN-22 07.00.00.016000000	PM 8 Y	N	
4	BRN_WORKHOURS_DET_4	OBPY_1	THU	4 01-JUN-22 09.00.00.362000000	AM 02-JUN-22 07.00.00.016000000	PM 8 Y	N	
5	BRN_WORKHOURS_DET_5	OBPY_1	FRI	5 01-JUN-22 09.00.00.362000000	AM 02-JUN-22 07.00.00.016000000	PM 8 Y	N	
6	BRN_WORKHOURS_DET_6	OBPY_1	SAT	6 01-JUN-22 09.00.00.362000000	AM 02-JUN-22 07.00.00.016000000	PM 8 Y	N	
7	BRN_WORKHOURS_DET_7	OBPY_1	SUN	7 (null)	(null)	8 N	N	

1.13 SLA Calculation

This topic describes the information about the SLA Calculation.

On initiation of workflow, plato-orch-service will create entries in below tables upon successful calculation of SLA for workflow and task.

ID	WORKFLOW_SLA_MASTER_ID	WORKFLOW_ID	TASK_ID	TASK_DEF_NA
1	e461ee49-b3b6-48cd-b351-f9ceaeef2c82	2279f604-873b-4df5-8807-1beb12dd6fea	eff113b-a52d-41ee-bcc8-0ff920bf8bc7	(null)
2	5da35c98-7d62-4e79-b239-ddc0043f857	2279f604-873b-4df5-8807-1beb12dd6fea	eff113b-a52d-41ee-bcc8-0ff920bf8bc7	MANUAL RETR
3	58924702-a344-435b-b3f4-c6e164a1e722	2279f604-873b-4df5-8807-1beb12dd6fea	eff113b-a52d-41ee-bcc8-0ff920bf8bc7	73a59578-6b0e-4e95-a0e2-6def10f2710a QuickInitiat
4	4a5aa2ea-5fc3-437b-8f21-c34823091094	2279f604-873b-4df5-8807-1beb12dd6fea	eff113b-a52d-41ee-bcc8-0ff920bf8bc7	af2df22b-d695-4744-aa9e-eac24df78063 Recommendation
5	57c3a339-5406-470d-8bd6-567e58af1d46	2279f604-873b-4df5-8807-1beb12dd6fea	eff113b-a52d-41ee-bcc8-0ff920bf8bc7	4785bcfe-4121-40ae-9514-eba5ba44c73e Approval
6	507c83ba-a5c5-4c93-afb5-3f9bafead0c85	2279f604-873b-4df5-8807-1beb12dd6fea	eff113b-a52d-41ee-bcc8-0ff920bf8bc7	4e577bb1-c02c-40cb-b055-ba23ba718d9a NYC
7	c81e876d-b8e4-4eeb-8a9d-ac4cf0f6c350	2279f604-873b-4df5-8807-1beb12dd6fea	eff113b-a52d-41ee-bcc8-0ff920bf8bc7	20dbec48-6027-4724-b728-94938782860b OnBoardingFr

	WORKFLOW_NAME	START_TIME	EXPECTED_COMPLETION	ACTUAL_COMPLETION	SUB_PROCESS_NAME	HOLD_FLAG	SUB_PROCESS_FLAG
1	CPOB	(null)	(null)	(null)	(null)	(null)	(null)
2	CPOB	06-JUN-22 10.27.49.000000000	AM 06-JUN-22 10.32.49.000000000	AM 06-JUN-22 10.36.23.126000000	AM (null)	(null)	(null)
3	CPOB	06-JUN-22 10.23.57.000000000	AM 06-JUN-22 10.28.57.000000000	AM 06-JUN-22 10.24.18.139000000	AM (null)	(null)	(null)
4	CPOB	06-JUN-22 10.36.23.000000000	AM 06-JUN-22 10.41.23.000000000	AM 06-JUN-22 10.45.06.062000000	AM (null)	(null)	(null)
5	CPOB	06-JUN-22 10.45.07.000000000	AM 06-JUN-22 10.50.07.000000000	AM 06-JUN-22 10.45.24.194000000	AM (null)	(null)	(null)
6	CPOB	06-JUN-22 10.24.18.000000000	AM 06-JUN-22 10.29.18.000000000	AM 06-JUN-22 10.24.43.920000000	AM (null)	(null)	(null)
7	CPOB	06-JUN-22 10.24.44.000000000	AM 06-JUN-22 10.29.44.000000000	AM 06-JUN-22 10.27.49.474000000	AM (null)	(null)	(null)

	_COMPLETION	SUB_PROCESS_NAME	HOLD_FLAG	SUB_PROCESS_FLAG	STATUS	PARALLEL_STAGE	HOLD_DURATION	BREACH_DURATION	BREACH_TIME
1		(null)	(null)	(null)	(null)	(null)	0	0	(null)
2	22	10.36.23.126000000	AM (null)	(null)	COMPLETED	(null)	0	5	06-JUN-22 10.32.49.000000000
3	22	10.24.18.139000000	AM (null)	(null)	COMPLETED	(null)	0	5	06-JUN-22 10.28.57.000000000
4	22	10.45.06.062000000	AM (null)	(null)	COMPLETED	(null)	0	5	06-JUN-22 10.41.23.000000000
5	22	10.45.24.194000000	AM (null)	(null)	COMPLETED	(null)	0	5	06-JUN-22 10.50.07.000000000
6	22	10.24.43.920000000	AM (null)	(null)	COMPLETED	(null)	0	5	06-JUN-22 10.29.18.000000000
7	22	10.27.49.474000000	AM (null)	(null)	COMPLETED	(null)	0	5	06-JUN-22 10.29.44.000000000

	ID	WORKFLOW_ID	WORKFLOW_NAME	INCLUDE_BRN_HLDY	INCLUDE_CURR_HLDY	INCLUDE_HOLD_TIME	INCLUDE_OFF_BRN
1	2279f604-873b-4df5-8807-1beb12ddfeaf	Eff113b-as24-41ee-bcc8-0ff920bf8bc7	CPOB	N	N	N	N

1.14 SLA Widgets

This topic describes the information about the SLA Widgets.

SLA Widgets provide a visual representation of party onboarding applications in different SLA statuses. SLA Widgets display the SLA status based on the SLA configuration for all different party types.

Total Onboarding Application Widget (Pie Chart)

A pie chart provides a high-level visual representation of all Party Onboarding applications in different SLA statuses. Following are the status supported by SLA Management.

- Within SLA – Green
- Near SLA Breach – Amber
- SLA Breached – Red

Total Onboarding Application Widget (Bar Chart)

A bar chart provides a visual representation of each party type for all party onboarding application in different SLA statuses. Following are the party types supported in bar chart:

- Retail
- Small and Medium Business
- Small and Medium Enterprise

- Corporate
- Financial Institution

SLA Status (Bar Chart)

A bar chart provides the task level visual representation for different SLA status.



Note:

SLA Widget only displays tasks which are not handed off to Back-office system.

To View SLA Widget:

1. From **Home** screen, click **Dashboard**.
The **Dashboard** screen displays.

View Details Filter

View Details filter in SLA widget provides a detailed view of party onboarding applications in different SLA statuses using the filter condition. Following filters can be used to search party onboarding application SLA statuses.

Table 1-18 SLA Widget – Field Description

Field	Description
Customer	Specify the Party ID of the customer.
Branch Code and Name	Specify the name of Branch onboarding the party.
Process	Specify the Party Onboarding Process Name.
From Date - To Date	Select the date criteria to search the party onboarding applications.
SLA Status	Select the SLA status as configured.

1.15 Dynamic Task Allocation

This topic describes the information about the Dynamic Task Allocation.

Dynamic Task allocation functionality distributes and assigns tasks to relevant user based on defined set of parameters. Once task is assigned to specific users, it is available in “My Tasks” for the user to take respective actions according to the stage of party onboarding process.

Dynamic Task allocation can be used by Financial Institutions to setup different rules for task allocation for different stages of party onboarding so that tasks are automatically assigned to authorized users.

Dynamic Task allocation is provided as Plato framework.

- [Setup Dynamic Task Allocation](#)
This topic describes the information to setup Dynamic Task Allocation.
- [Task Allocation Process](#)
This topic describes the information about the Task Allocation Process.

- [Postman Collection for Rules APIs](#)
This topic describes the information about the Postman Collection for Rules APIs.

1.15.1 Setup Dynamic Task Allocation

This topic describes the information to setup Dynamic Task Allocation.

- [Plato Configuration](#)
This topic describes the systematic instructions to configure the Plato for Dynamic Task Allocation.
- [Fact Creation](#)
This topic describes the systematic instructions to create the Facts required for Dynamic Task Allocation.
- [Rule Creation](#)
This topic describes the systematic instructions to create the Rules required for Dynamic Task Allocation.
- [Rule Group Creation](#)
This topic describes the systematic instructions to create the Rule Groups required for Dynamic Task Allocation.
- [Entry in TASK_CONFIG table](#)
This topic describes the systematic instruction to create an entry in TASK_CONFIG table.

1.15.1.1 Plato Configuration

This topic describes the systematic instructions to configure the Plato for Dynamic Task Allocation.

1. Parameter `-Dplato.orchestrator.enableDynamicAllocation=true` should be added in server start for Plato Managed Server.

The screenshot shows the Oracle WebLogic Server Administration Console for the 'plato-Orcn_manageoserver'. The 'Server Start' tab is active. The 'Arguments' field contains the following text:

```
Dplato.cmc.default.user=ADMINUSER1 -
Dplato.cmc.default.brn=000 -
Dplato.orchestrator.enableSLA=false -
Dplato.orchestrator.enableDynamicAllocation=true -
Dmulti.entity.enabled=true
```

2. Restart Plato Managed Server.

 **Note:**

Check the following PROPERTIES table in PLATO schema as sometimes the value may be overridden.

- plato.orchestrator.enableDynamicAllocation should be set to TRUE
- plato.orchestrator.usingRuleEngine should be set to TRUE

34	4724	plato-orch-service	jdbc	jdbc	plato.cmc.default.user	ADMINUSER1
35	4725	plato-orch-service	jdbc	jdbc	plato.orchestrator.enableDynamicAllocation	true
36	4726	plato-orch-service	jdbc	jdbc	plato.orchestrator.enableSLA	true
37	5497	plato-orch-service	jdbc	jdbc	plato.orchestrator.enableSubWfDynamicAllo...	false
38	60	plato-orch-service	jdbc	jdbc	plato.orchestrator.uri	https://tempval/plato-orc
39	4841	plato-orch-service	jdbc	jdbc	plato.orchestrator.usingRuleEngine	true

1.15.1.2 Fact Creation

This topic describes the systematic instructions to create the Facts required for Dynamic Task Allocation.

The following FACTS are supported out-of-box

- Priority
- applicationDate
- applicationNumber
- processRefNumber
- amount (for Loans and Credit Card)
- currencyCodebranch
- currentBranch
- user (initiated by user)
- customerNumber
- processName
- processCode
- stage
- lifecycleCode
- businessProductCode

Other facts (using data elements from any of the Data Segments) can be derived by using http task. Facts can be created on any of the input parameters from Task for each Stage.

Initiate the FACT Creation

1. On **Home** screen, click **Rule**. Under **Rule**, click **Fact**.
2. Under **Fact**, click **Create Fact**.

The **Create Fact** screen displays.

Figure 1-25 Create Fact

 **Note:**

For more information on Fact Creation, refer to the **Rule Framework** section in **Oracle Banking Common Core User Guide**.

1.15.1.3 Rule Creation

This topic describes the systematic instructions to create the Rules required for Dynamic Task Allocation.

Rules can be defined as per financial institutions requirements for Dynamic Task Allocation. Based on the rules, tasks can be assigned dynamically to different users.

Initiate the Rule Creation

1. On **Home** screen, click **Rule**. Under **Rule**, click **Rule**.
2. Under **Rule**, click **Create Rule**.

The **Create Rule** screen displays.

Figure 1-26 Create Rule Group

Supported Outputs for Rules

In the current framework, the following rule outputs are supported.

Table 1-19 Supported Outputs for Rules

Output Type	Format	Description
USER	USER:<user name>	This output type for a rule is simple and it means that whatever username is provided for the rule the same user will be allocated the task if rule is satisfied.
FIELD	FIELD:<field from conductor task>	This type of output means that whatever is the value of the field, which is part of conductor input parameter, that field value (must be a username) will be assigned the task after satisfying the rule.

 **Note:**

For more information on Rule Creation, refer to the **Rule Framework** section in **Oracle Banking Common Core User Guide**.

1.15.1.4 Rule Group Creation

This topic describes the systematic instructions to create the Rule Groups required for Dynamic Task Allocation.

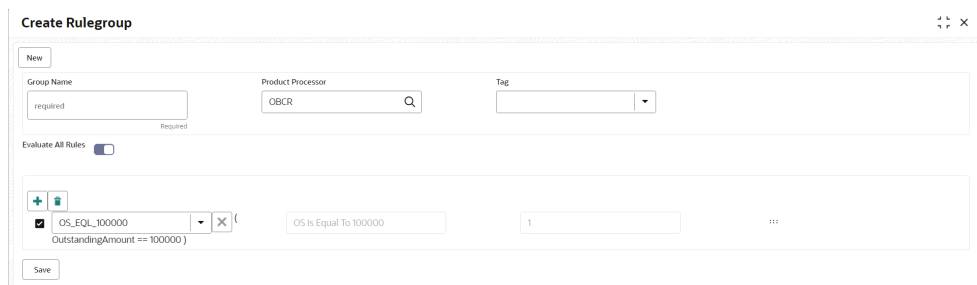
Rule group Maintenance will be used for prioritizing the rules. The rule will be run as per the priority, and if the condition is met, assignment will happen to the user per the rule outcome. If none of the rule is met, then task will not be assigned to a user (task will be unassigned and available under “Free tasks”)

Initiate the Rule Group Creation

1. On **Home** screen, click **Rule**. Under **Rule**, click **Rule Group**.
2. Under **Rule Group**, click **Create Rule Group**.

The **Create Rule Group** screen displays.

Figure 1-27 Create Rule Group





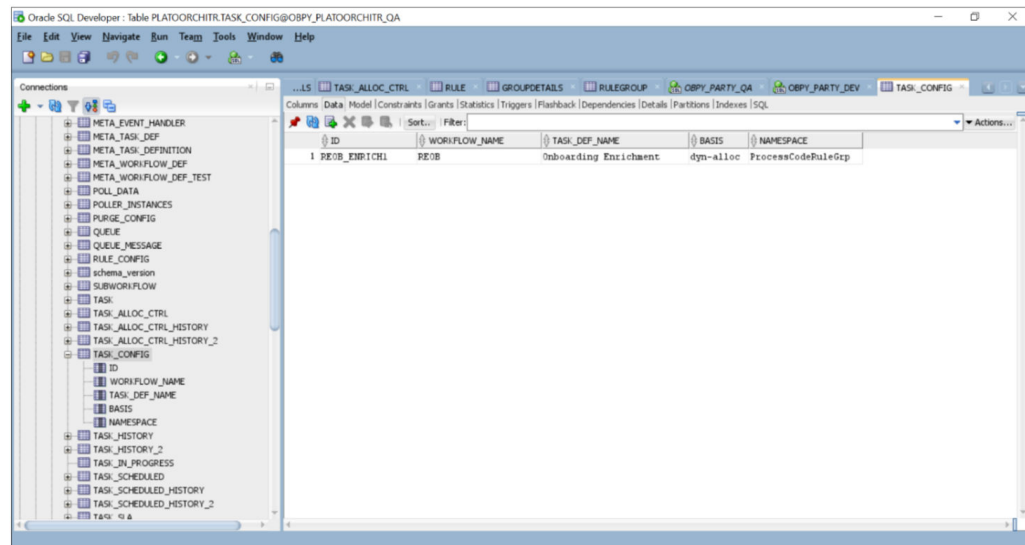
1.15.1.5 Entry in TASK_CONFIG table

This topic describes the systematic instruction to create an entry in TASK_CONFIG table.

Create entry in TASK_CONFIG table in PLATOORCHITR schema as follows:

Table 1-20 TASK_CONFIG - Table Description

Name	Description
ID	Specify the Unique Identifier in Task_Config table.
WORKFLOW_NAME	Specify the name of the workflow for which dynamic task allocation must be done. <div data-bbox="906 657 1463 863" style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> Note:</p> <p>WORKFLOW_NAME can be taken from HTASK_ADDN_DTLS table for respective workflow and stages.</p> </div>
TASK_DEF_NAME	Specify the Task definition name of the task for which dynamic task allocation must be done. <div data-bbox="906 999 1463 1205" style="border-left: 2px solid #0070C0; padding-left: 10px; margin-top: 10px;"> <p> Note:</p> <p>TASK_DEF_NAME can be taken from HTASK_ADDN_DTLS table for respective workflow and stages.</p> </div>
BASIS	Hardcoded to dyn-alloc
NAMESPACE	Specify the name of the Rule Group which has the rule which will be invoked and evaluated during dynamic task allocation.



Note:

Restart Rule Service after the above configuration is completed.

1.15.2 Task Allocation Process

This topic describes the information about the Task Allocation Process.

Once the task is created as per the business process, if there is any user assignment linked for a stage, the system will log the relevant tasks in a table for allocation. A poller runs on this table and execute the Rules linked in the allocation maintenance. Rules will be executed one after another as per the priority set. If priority 1 rule is met, it will give a user as an outcome, the system will do the user assignment as per the assignment method defined in the assignment code. Its criteria in Rule 1 are not met, it will go to next rule (priority 2) and so on. If all the Rules are exhausted without meeting the conditions, the task will remain as unassigned to any user.

If there are no user assignment codes linked to any stages, then also, the task will remain unassigned to any user.

To check Task Allocation process, start new Retail Onboarding and Go till Enrichment stage to check whether the task is getting allocated to user defined in Rule Output.

If the Rule Evaluation is successful, a Task will be allocated to User in TASK_ALLOC_CTRL table.

To view Task assignment to respective users, check **My Tasks** section of the respective user.

1.15.3 Postman Collection for Rules APIs

This topic describes the information about the Postman Collection for Rules APIs.

Download [plato-rule.postman_collection.json](#) file and refer the postman collection for Rules REST endpoint APIs.

1.16 Multi-Level Authorization

This topic describes the information about the Multi-Level Authorization.

Multi-level authorization functionality provides a flexibility to configure more than one reviewer and approver during different party onboarding processes. Multi-level authorization allows user to capture review and approval comments and decision for a party onboarding process.

- [Setup Multi-Level Authorization](#)
This topic describes the information to setup Multi-Level Authorization.
- [Additional Field Configuration](#)
This topic describes the information about the Additional Field Configuration.
- [Upload Source for Common Core \(CMC\) Party Replication](#)
This topic describes the information about the Upload Source for Common Core (CMC) Party Replication.

1.16.1 Setup Multi-Level Authorization

This topic describes the information to setup Multi-Level Authorization.

Changes in Process Flow (All Party types)

1. In Retail and SMB process-flows, Review stage is renamed as Recommendation stage.
2. Common Review, Recommendation and Approval UI screens and corresponding services (Backend service definition and tables) are created for all party types.
3. New tables created for Review, Recommendation and Approval stages is as follows:
 - OBPY_TB_PRTY_REVIEW_MSTR
 - OBPY_TB_PRTY_REVIEW_DETAILS
 - OBPY_TB_PRTY_REVIEW_DTLS_LIST
4. New Sub-workflows is created for Recommendation and Approval stages with single task in each stage.
Download the `Approval_SubWorkflow.json` and `Recommendation_SubWorkflow.json` sub-workflow files for reference.

 **Note:**

Sub-workflow definition created here has only one task/stage in the sub-workflow.

5. Sub-workflow definition must be updated in below endpoint in each environment:
`plato-orch-service/api/metadata/workflow`

Sample CURL for the endpoint is as follows:

```
curl --location --request POST 'https://ofss-  
mum-753.snbomprshared1.gbucdsint02bom.  
oraclevcn.com:6008/plato-orch-service/api/metadata/workflow' \  
--header 'Accept: application/json' \  
--header 'appId: platoorch' \  

```

```
--header 'Authorization: Bearer {{token}}' \
--header 'authToken: token' \
--header 'branchCode: 000' \
--header 'Connection: keep-alive' \
--header 'Content-Type: application/json' \
--header 'userId: SASIKALA' \
--header 'entityId: DEFAULTENTITY' \
--data-raw '' à Sub-workflow definition
```

6. After the request is posted with 201 Created HTTP status, workflow definition can be checked in PLATOORCH schema table: **META_WORKFLOW_DEF** table.
Definition of **META_WORKFLOW_DEF** table:

ID -> Unique_id

CREATED_ON -> created date timestamp

MODIFIED_ON -> modified date timestamp

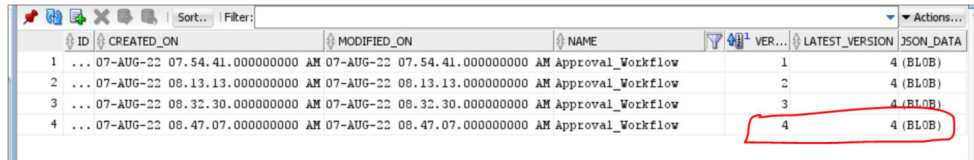
NAME -> Process-code . For eg: REOB, CPOB, Approval_Sub_Workflow etc

VERSION -> version number

LATEST_VERSION -> latest version number

JSON_DATA -> workflow definition

The following screenshot of **META_WORKFLOW_DEF** table after sub-workflow is created through REST endpoint:



ID	CREATED_ON	MODIFIED_ON	NAME	VER...	LATEST_VERSION	JSON_DATA
1	07-AUG-22 07.54.41.0000000000 AM	07-AUG-22 07.54.41.0000000000 AM	Approval_Workflow	1	4	(BLOB)
2	07-AUG-22 08.13.13.0000000000 AM	07-AUG-22 08.13.13.0000000000 AM	Approval_Workflow	2	4	(BLOB)
3	07-AUG-22 08.32.30.0000000000 AM	07-AUG-22 08.32.30.0000000000 AM	Approval_Workflow	3	4	(BLOB)
4	07-AUG-22 08.47.07.0000000000 AM	07-AUG-22 08.47.07.0000000000 AM	Approval_Workflow	4	4	(BLOB)

7. The Changes is done in process-flow for Recommendation and Approval stages.

BEFORE:

Review task:

```
{
  "name": "Review",
  "taskReferenceName": "Retail_Review",
  "inputParameters": {
    "FUNCTIONAL_CODE": "OBPY_FA_REOB_REVIW",
    "applicationDate": "$
{workflow.input.txnIdentification.taskCreationDate}",
    "applicationNumber": "$
{workflow.input.txnIdentification.moduleCode}",
    "customerNumber": "$
{workflow.input.transactionData.moduleData.customerId}",
    "processName": "Retail Onboarding",
    "partyId": "$
{workflow.input.transactionData.moduleData.customerId}",
    "productCode": "$
{workflow.input.transactionData.moduleData.productCode}",
    "processRefNumber": "$
```

```

{workflow.input.txnIdentification.processRefNo}",
  "processCode": "REOB",
  "branch": "${workflow.input.txnIdentification.branchCode}",
  "stageId": "OBPY_FA_REOB_REVIW",
  "priority": "${workflow.input.txnIdentification.taskPriority}",
  "instanceId": "${workflow.input.instanceId}",
  "stage": "Review",
  "TASK_OUTCOMES": ["PROCEED", "ADDITIONAL_INFO", "MANUALRETRY"]},
  "type": "WAIT",
  "startDelay": 0,
  "optional": false,
  "asyncComplete": fals
}

```

Review task:

```

{
  "name": "Approval",
  "taskReferenceName": "Retail_Approval",
  "inputParameters": {
    "FUNCTIONAL_CODE": "OBPY_FA_REOB_APPRL",
    "applicationDate": "${
{workflow.input.txnIdentification.taskCreationDate}",
    "applicationNumber": "${
{workflow.input.txnIdentification.moduleCode}",
    "customerNumber": "${
{workflow.input.transactionData.moduleData.customerId}",
    "processName": "Retail Onboarding",
    "partyId": "${
{workflow.input.transactionData.moduleData.customerId}",
    "productCode": "${
{workflow.input.transactionData.moduleData.productCode}",
    "processRefNo": "${workflow.input.txnIdentification.processRefNo}",
    "processRefNumber": "${
{workflow.input.txnIdentification.processRefNo}",
    "processCode": "REOB",
    "branch": "${workflow.input.txnIdentification.branchCode}",
    "stageId": "OBPY_FA_REOB_APPRL",
    "priority": "${workflow.input.txnIdentification.taskPriority}",
    "instanceId": "${workflow.input.instanceId}",
    "stage": "Approval",
    "TASK_OUTCOMES": ["PROCEED", "REJECT", "ADDITIONAL_INFO",
"MANUALRETRY"]
  },
  "type": "WAIT", "startDelay": 0,
  "optional": false,
  "asyncComplete": false
}

```

AFTER:

Recommendation task:

```

{
  "name": "Recommendation_Subwf",
  "taskReferenceName": "Recommendation_Subwf",
  "inputParameters": {
    "FUNCTIONAL_CODE": "OBPY_FA_REOB_RECOM",
    "applicationDate": "$
{workflow.input.txnIdentification.taskCreationDate}",
    "applicationNumber": "$
{workflow.input.txnIdentification.moduleCode}",
    "customerNumber": "$
{workflow.input.transactionData.moduleData.customerId}",
    "processName": "Retail Onboarding",
    "partyId": "$
{workflow.input.transactionData.moduleData.customerId}",
    "productCode": "$
{workflow.input.transactionData.moduleData.productCode}",
    "processRefNumber": "$
{workflow.input.txnIdentification.processRefNo}",
    "processCode": "REOB",
    "branch": "${workflow.input.txnIdentification.branchCode}",
    "priority": "${workflow.input.txnIdentification.taskPriority}",
    "moduleCode": "${workflow.input.txnIdentification.productCode}",
    "instanceId": "${workflow.input.instanceId}",
    "stageId": "OBPY_FA_REOB_RECOM",
    "stage": "Recommendation"
  },
  "type": "SUB_WORKFLOW",
  "subWorkflowParam": {
    "name": "Recommendation_Workflow",
    "version": 1
  }
}

```

Approval task:

```

{
  "name": "Approval_Subwf",
  "taskReferenceName": "Retail_Approval_Subwf",
  "inputParameters":
  {
    "FUNCTIONAL_CODE": "OBPY_FA_REOB_APPRL",
    "applicationDate": "$
{workflow.input.txnIdentification.taskCreationDate}",
    "applicationNumber": "$
{workflow.input.txnIdentification.moduleCode}",
    "customerNumber": "$
{workflow.input.transactionData.moduleData.customerId}",
    "processName": "Retail Onboarding",
    "partyId": "$
{workflow.input.transactionData.moduleData.customerId}",
    "productCode": "$
{workflow.input.transactionData.moduleData.productCode}",

```

```

    "processRefNo": "${workflow.input.txnIdentification.processRefNo}",
    "processRefNumber": "${
{workflow.input.txnIdentification.processRefNo}",
    "processCode": "REOB",
    "branch": "${workflow.input.txnIdentification.branchCode}",
    "priority": "${workflow.input.txnIdentification.taskPriority}",
    "moduleCode": "${workflow.input.txnIdentification.productCode}",
    "instanceId": "${workflow.input.instanceId}",
    "stageId": "OBPY_FA_REOB_APPRL",
    "stage": "Approval"
},
    "type": "SUB_WORKFLOW",
    "subWorkflowParam": {
        "name": "Approval_Workflow",
        "version": 1
    }
}

```

Things to be Updated in process-flows definition

1. When any new sub-workflow is added, to inject it into the main process-flow new task must be created as SUB-WORKFLOW and subWorkflowParam must be updated with appropriate version of sub-workflow.
2. Latest version of the sub-workflow must be checked in META_WORKFLOW_DEF table and the same must be updated in subWorkflowParam version for any new changes in sub-workflow definition.
3. To enable multi-level authorization (For example multiple review and approval stages) below changes must be done:
 - a. Sub-workflow must be updated with multiple tasks. Based on requirement, it can be updated with parallel tasks (FORK-JOIN task) or sequential tasks (WAIT task).
 - b. Main process-flow must be updated with latest version of sub-workflow.
 - c. Both Sub-workflow and Main process-flow must be updated in META_WORKFLOW_DEF table through REST endpoint.

1.16.2 Additional Field Configuration

This topic describes the information about the Additional Field Configuration.

Scenario: Adding additional fields to a new Data Segment and add it to the train hop

Step 1: Add Metadata in additional attributes common core maintenance. Post maintenance the entry in CMC_TM_ADDDT_ATTR_MASTER should be as follows:

Table 1-21 CMC_TM_ADDT_ATTR_MASTER - Entry Values

ID	UI_KEY	Description	FIELD_META_DATA
1	fsgbu-ob-cmn-ds-additional-fields@OBPY_REOB_ENRH	Additional fields for REOB process	[{ "id": "UDF_TEXTATTR", "label": "Text", "type": "TEXT" }, { "id": "UDF_NUMBERATTR", "label": "Number", "type": "NUMBER" }, { "id": "UDF_TEXTAREAATTR", "label": "TextArea", "type": "TEXTAREA" }, { "id": "UDF_DATEATTR", "label": "Date", "type": "DATE" }, { "id": "UDF_DROPDOWNATTR", "label": "Dropdown", "value": "A", "type": "DROPDOWN", "options": [{ "value": "A", "label": "A" }, { "value": "U", "label": "U" }] }, { "id": "UDF_SWITCHATTR", "label": "Switch", "value": true, "type": "SWITCH" }, { "id": "UDF_LOVATTR", "label": "Customer", "type": "LOV", "lovId": "customerLOV" }]

 **Note:**

- Values in UI_KEY column refers to a unique identification reference key of any screen
- Sample metadata has been given in the Field_meta_data column. In the example a field of type text has been defined with Id - UDF_TEXTATTR. Similarly type – Number, textarea, dropdown, lov and switch has been added

Step 2: Configure the train hop entries with the CCA Name for OBPY using **Business Process** screen.

OBPY UI:

CCA - fsgbu-ob-py-ds-additional-attributes is in OBPY component server to serve this purpose.

Service:

The payload with the additionalAttributes json will be processed on next click in UI for the above CCA.

Step 3: Handoff Changes

- A property in obpy-properties table is made available with the key REOB_ADDITIONAL_FIELDS_UIKEY, and the respective value holds the UI key of the core maintenance.
- REOB_ADDITIONAL_FIELDS_UIKEY can accept multiple UI keys for handoff and the values should be pipe ('|') separated (if additional attributes are added in multiple screens for a single process).
- All the additional fields captured in different data segments for a single process and configured in above property will be collated and passed on as UDF label, value list and will be available in the OBRH Request.
- UDF json will be appended to the party JSON which is ready for handoff and can be mapped to the request template through OBRH for the HOST. Template changes are available in the request transformation:

```
#foreach($UDF in $body.UDFList)
  <fcub:UDFDETAILS>
  <fcub:FLDNAM>$UDF.label</fcub:FLDNAM>
  <!--Optional:-->
  <fcub:FLDVAL>$UDF.value</fcub:FLDVAL>
</fcub:UDFDETAILS>
#end
```

- Once after the FCUBS handoff, the UDF fields will be handed off and can be checked in STDCIF screen - Fields tab

1.16.3 Upload Source for Common Core (CMC) Party Replication

This topic describes the information about the Upload Source for Common Core (CMC) Party Replication.

On completion of party onboarding process and party details handoff to FLEXCUBE Universal Banking (FCUBS), customer information along with CIF ID (FCUBS) is replicated to Common Core in **External Customer**.

For Party replication to Common Core (CMC), the upload source should be configured in FCUBS and Common Core.

 **Note:**

- For more information on Upload Source configuration in FCUBS, refer to **FLEXCUBE Universal Banking - Party Services Integration Guide**.
- For more information on Upload Source configuration in Common Core, refer to **Oracle Banking Common Core User Guide**.

1.17 Regional Configuration

Regional configuration framework is provided by Plato to enable and configure products within the Oracle Banking Microservices Architecture framework as per regional requirements.

Oracle Banking Party uses the regional framework to configure the following parameter type as per the regional configuration.

Table 1-22 Use - Case for Regional Configuration

Features	Use - Case
Mandatory – Yes/No	Some UI fields in Party will be mandatory in some geographies while others maybe mandatory in other geographies. Using the regional framework, the optional fields in the base product can be made mandatory.
Field Visibility – Yes/No	Some UI fields in Party will be visible in some geographies while others maybe visible in other geographies. Using the regional framework, the optional fields in the base product can be made visible or hidden.
Data Type Validation (Regular Expression)	Using regional framework, a field can be validated for field input like identity number to accept only numeric value upto 9 numbers.
Default Value	Using regional framework, field input can be default on launch of a screen like country code as US in Country of Resident field.
Field Label	Using regional framework, field label can be changed as per generic convention in a specific region such as Resident Status change to Citizenship status in US region.

To configure the regional configuration for Oracle Banking Party, the following Plato tables need to be inserted along with the required configuration.

Figure 1-28 PLATO_REGIONAL_TM_CONFIG_MASTER Table

REGION_CODE	MODULE_CODE	IS_REGIONALIZATION_ENABLED	IS_SCREEN_REG_ENABLED	IS_SCREEN_VALIDATION_REG_ENABLED
US	REPORTSERVICE	Y	Y	N
IN	REPORTSERVICE	Y	Y	N
US	PLATOFEEED	Y	N	N
IN	PLATOFEEED	Y	Y	Y

The description for the columns in the above image are explained below:

- For a particular REGION_CODE, there can be multiple MODULE_CODE (app Ids) as mentioned in the PLATO_REGIONAL_TM_CONFIG_MASTER table.
- Maintain a value 'Y' in the IS_REGIONALIZATION_ENABLED flag for regionalization and troubleshooting.
- To enable screen regionalization, maintain a value 'Y' in the IS_SCREEN_REG_ENABLED flag.

 **Note:**

If the IS_SCREEN_REG_ENABLED flag is maintained as 'N' and the IS_REGIONALIZATION_ENABLED flag is maintained as 'Y' then the regional fields do not appear on the screen and label changes will not reflect.

- To enable the service side validations, maintain a value as 'Y' in the IS_SCREEN_VALIDATION_REG_ENABLED flag.

Figure 1-29 PLATO_REGIONAL_TM_SCREEN_CONFIG Table

REGION_CODE	MODULE_CODE	CCA_NAME	FIELD_ID	IS_MANDATORY	IS_VISIBLE	DEF_VALUE	PATTERN
IN	REPORTSERVICE	fagbu-ob-reports-mn	cnt	Y	Y		
US	REPORTSERVICE	fagbu-ob-reports-mn	outformat	Y	Y	PDF	
US	REPORTSERVICE	fagbu-ob-reports-mn	text-area	Y	Y		[a-zA-Z]{3}
IN	REPORTSERVICE	fagbu-ob-reports-mn	outformat	Y	Y	PNG	
IN	REPORTSERVICE	fagbu-ob-reports-mn	name	Y	Y		[a-zA-Z]{5}
US	REPORTSERVICE	fagbu-ob-reports-mn	state	Y	Y		

The description for the columns in the above image are explained below:

- For a particular REGION_CODE, there can be multiple MODULE_CODE (app Ids) as mentioned in the PLATO_REGIONAL_TM_CONFIG_MASTER table.
- Maintain the name of the CCA in the CCA_NAME for the particular regional field belongs.
- Maintain the ID attribute of the regional field in the FIELD_ID column.
- To enable the regional field, maintain the value as "Y" in the IS_MANDATORY column.
- To configure the visibility of the regional field, maintain the value as 'Y' in the IS_VISIBLE column.
- Update the DEF_VALUE column to display the default value (when the screen launches) in the regional field.
- The regExp pattern based on which UI validation should happen, should be maintained in the PATTERN column.

Glossary

Index

A

Address Management, [1-2](#)

C

Configurations, [1-1](#)

Create Credit Agency, [1-5](#)

Customer Access Group, [1-13](#)

D

Dynamic Task Allocation, [1-28](#)

E

Entity Maintenance, [1-6](#)

H

Host Configuration, [1-8](#)

L

Location Maintenance, [1-9](#)

M

Mask Maintenance, [1-10](#)

Multi-Level Authorization, [1-35](#)

O

Organization Maintenance, [1-12](#)

P

PII Masking Maintenance, [1-15](#)

Properties Maintenance, [1-19](#)

S

Service Level Agreements, [1-23](#)

Setup Service Level Agreements, [1-23](#)

SLA Calculation, [1-26](#)

SLA Widgets, [1-27](#)

System Maintenance, [1-21](#)

V

View Credit Agency, [1-6](#)