

Oracle Banking Party Configurations User Guide

Oracle Banking

Release 14.6.0.0.0

Part Number F57244-01

May 2022

Oracle Banking Party Configurations User Guide

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

<https://www.oracle.com/industries/financial-services/index.html>

Copyright © 2021, 2022, 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.

Contents

1	Preface	1
1.1	Introduction.....	1
1.2	Audience.....	1
1.3	Document Accessibility	1
1.4	Acronyms and Abbreviations	1
1.5	List of Topics.....	1
1.6	Related Documents	2
1.7	Symbols and Icons.....	2
1.8	Basic Actions	3
2	Configurations.....	4
2.1	Customer Access Group.....	4
2.2	PII Masking Maintenance.....	6
2.3	Entity Maintenance	11
2.4	Location Maintenance.....	13
2.5	Mask Maintenance.....	15
3	List of Menus	18

1 Preface

1.1 Introduction

This guide provides step-by-step instructions for Configuration Maintenance in Oracle Banking Party.

1.2 Audience

The user 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

1.3 Document 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>.

1.4 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 Table

Abbreviation	Description
PII	Personally Identifiable Information

1.5 List of Topics

This guide is organized as follows:

Table 2: List of Topics

Topics	Description
Configuration Maintenance	This topic provides an overview of the Configuration Maintenance in Oracle Banking Party and covers the actions to be performed during Configuration Maintenance
List of Glossary	This topic displays the list of main screens in the document along with its reference.

1.6 Related Documents






The related documents are as follows:

1. Getting Started User Guide
2. Oracle Banking Common Core User Guide
3. Oracle Banking Security Management System User Guide

1.7 Symbols and Icons

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

Table 3: Symbols and Icons

Symbol	Description
→	Represents Results
	Add icon
	Edit icon
	Delete icon
	Calendar icon
	Close icon

1.8 Basic Actions

Most of the screens contain buttons to perform all or few of the basic actions. The table below 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 & Close	On click of Save & Close, the captured details will be saved. If mandatory fields have not been captured, system will display error until the mandatory fields are captured.

2 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.

This topic contains the following sub-topics:

- [2.1 Customer Access Group](#)
- [2.2 PII Masking Maintenance](#)
- [2.3 Entity Maintenance](#)
- [2.4 Location Maintenance](#)
- [2.5 Mask Maintenance](#)

Prerequisites:

Specify **User Id** and **Password**, and login to **Home screen**.

Refer to **Getting Started User Guide** for the login procedure.

2.1 Customer Access Group

Customer access group functionality is part of privacy by design requirements. 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 below.

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

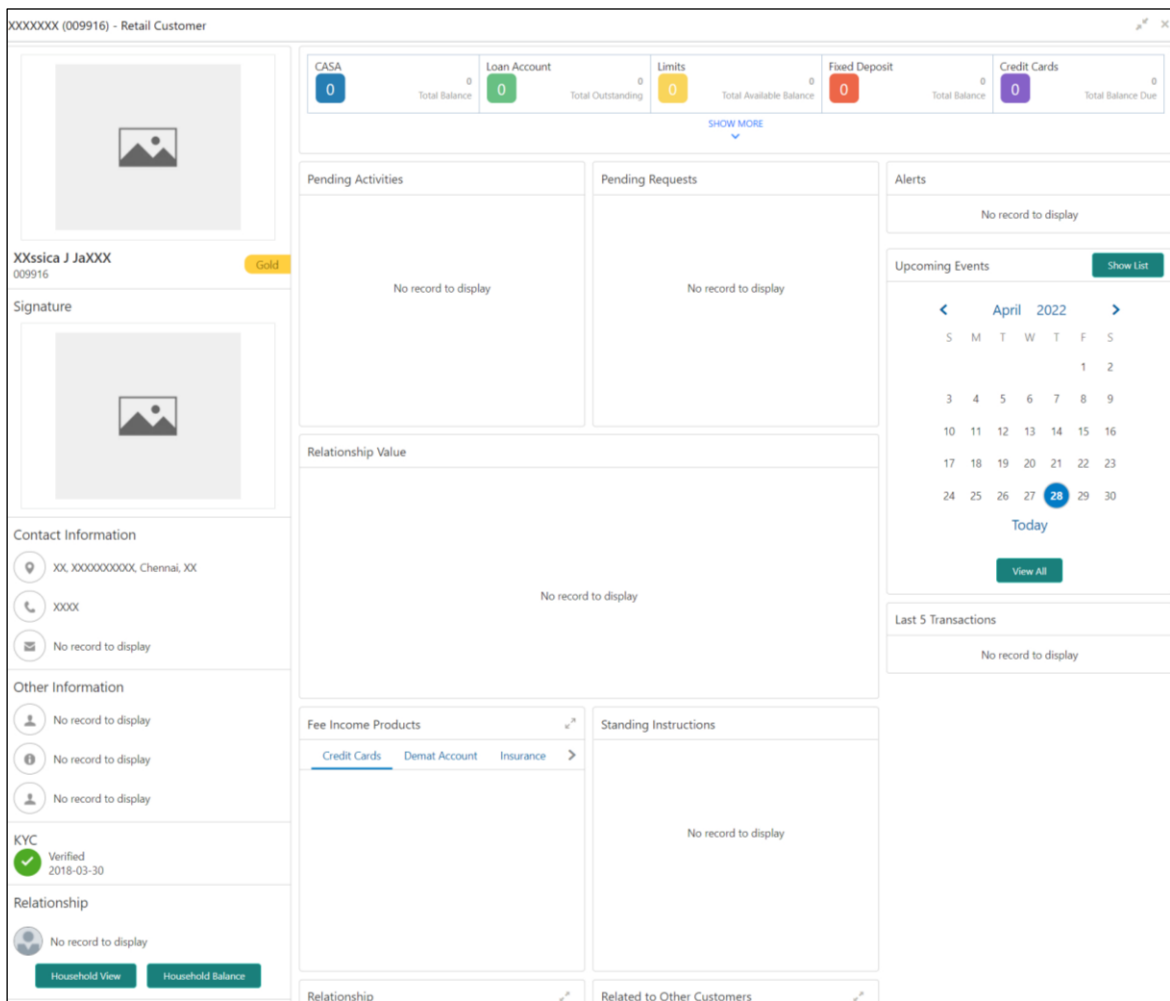
2.2 PII Masking Maintenance

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: Sample Masked Information



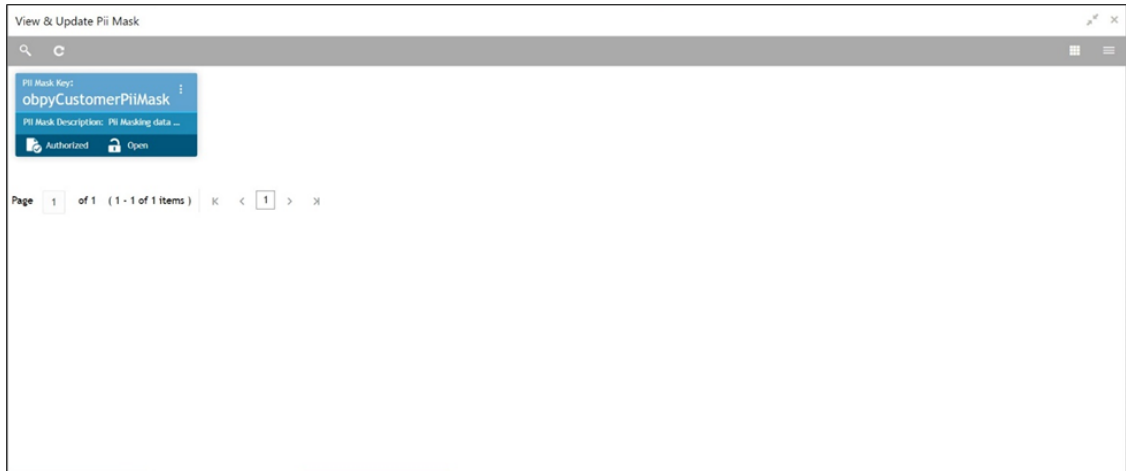
Refer to **Oracle Banking Security Management System User Guide** for more details on enabling and disabling PII access for the user.

To 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 is displayed.

Figure 2: View and Update PII Mask



3. Click **Unlock**.

→ The **Create PII Mask** screen is displayed.

Figure 3: Create PII Mask

Attribute Name	Data Type	Data Length	Mask Enable	Mask Character	Mask Entire Field	First N Characters	Last N Characters	Action
Title	String	36	N	X	Y	0	0	
First Name	String	255	Y	X	N	2	1	
Middle Name	String	255	Y	X	Y	0	0	
Last Name	String	255	Y	X	N	1	0	
Short Name	String	36	Y	X	Y	0	0	
Maiden Name	String	255	Y	X	Y	0	0	
Name In Local Language	String	255	N	X	Y	0	0	
Date of Birth	Date		Y	1970-01-01	Y			
Gender	String	255	Y	X	Y	0	0	

4. On **Create PII Mask** screen, select **PII Group**.

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

Table 5: Create PII Mask – Field Description

Field	Description
<p>PII Group</p>	<p>Select the Logical grouping of PII Fields in the dropdown list.</p> <p>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

5. The List of PII fields will be available in table structure as per selected **PII group**.
6. Click **Action** button for configuring Mask for each individual PII field.
 → The **Edit PII Masking** screen is displayed.

Figure 4: Edit PII Masking

The screenshot shows a window titled "Edit PII Masking" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Attribute Name:** Title
- Data Type:** String
- Data Length:** 36
- Mask Enable:** A toggle switch that is currently turned off.
- Mask Character:** X
- Mask Entire Field:** A toggle switch that is currently turned on.
- First N Characters:** A numeric input field with up and down arrows, set to 0.
- Last N Characters:** A numeric input field with up and down arrows, set to 0.
- Buttons:** "Update" and "Cancel" buttons are located at the bottom right of the dialog.

7. On **Edit PII Masking** screen, specify the required details in the respective fields and click **Update**.

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

Table 6: Edit PII Masking – 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	<p>Select the toggle to identify whether the masking is enabled or disabled for the field.</p> <p>If Mask Enable toggle is ON, the field will be displayed as masked to unauthorized users.</p> <p>If Mask Enable toggle is set as OFF, the field will display without masking to all users.</p>
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 masking configuration for all required PII fields.

Once the record is authorized by the checker,

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

→ The **View and Update PII Mask** screen is displayed.

Figure 5: View and Update PII Mask



11. Click **View** to view the defined PII masking.

→ The **View Mask** screen is displayed.

Figure 6: View Mask

Attribute Name	Data Type	Data Length	Mask Enable	Mask Character	Mask Entire Field	First N Characters	Last N Characters
Title	String	36	N	X	Y	0	0
First Name	String	255	Y	X	N	2	1
Middle Name	String	255	Y	X	Y	0	0
Last Name	String	255	Y	X	N	1	0
Short Name	String	36	Y	X	Y	0	0
Maiden Name	String	255	Y	X	Y	0	0
Name In Local Language	String	255	N	X	Y	0	0
Date of Birth	Date		Y	1970-01-01	Y		
Gender	String	255	Y	X	Y	0	0
Marital Status	String	255	N	X	Y	0	0
Unique ID	String	36	Y	X	Y	0	0
Birth Country	String	255	Y	X	Y	0	0
Nationality	String	255	N	X	Y	0	0
Citizenship by	String	255	N	X	Y	0	0
Resident Status	String	255	N	X	Y	0	0
Country of residence	String	255	N	X	Y	0	0
Location	String	255	N	X	Y	0	0
Preferred Language	String	255	N	X	Y	0	0

2.3 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 user will be able to

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

To initiate Entity Maintenance

1. From **Home screen**, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Entity**. Under **Entity**, click **Create Entity**.

→ The **Create Entity** screen is displayed.

Figure 7: Create Entity


3. On **Create Entity** screen, specify the following attributes.

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

Table 7: 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.
Sub Entity Code	Specify the Sub Entity Code for the selected Entity Code.

Field	Description
Sub Entity Description	Specify the description of Sub Entity Code.

4. Click  button to add Sub-entities for Entity Code.

5. Click **Save**.

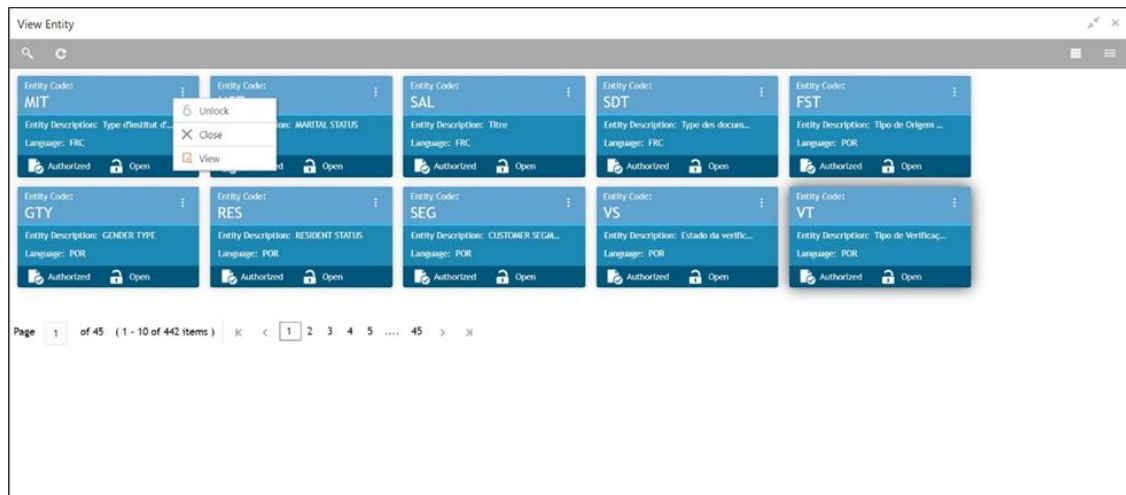
Once the record is authorized by the checker,

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

7. Under **Maintenance**, click **Entity**. Under **Entity**, click **View Entity**.

→ The **View Entity** screen is displayed.

Figure 8: View Entity



2.4 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.

To Initiate Location Maintenance

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

→ The **Create Location** screen is displayed.

Figure 9: Create Location

3. On **Create Location** screen, specify the following attributes.

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

Table 8: 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.

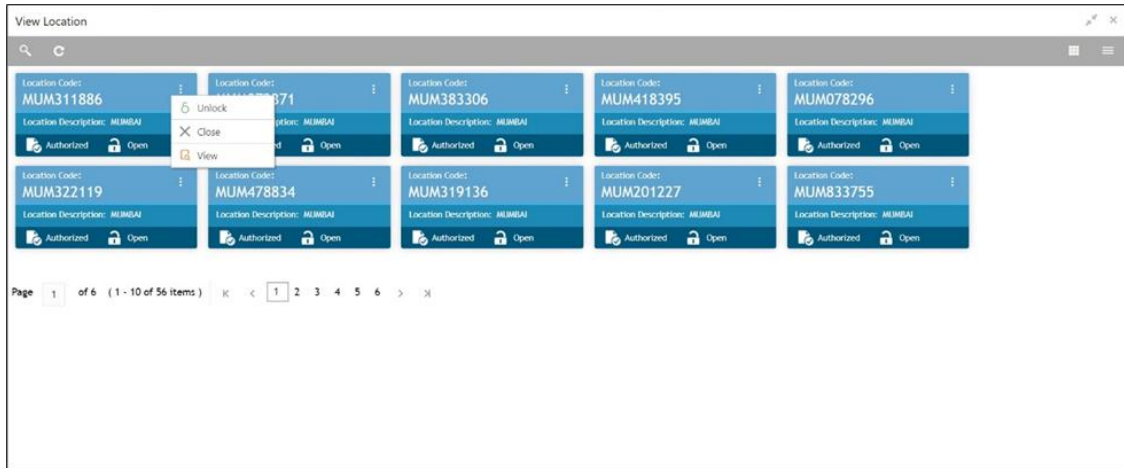
4. Click **Save** to save the location code.

Once the record is authorized by the checker,

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 is displayed.

Figure 10: View Location



2.5 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

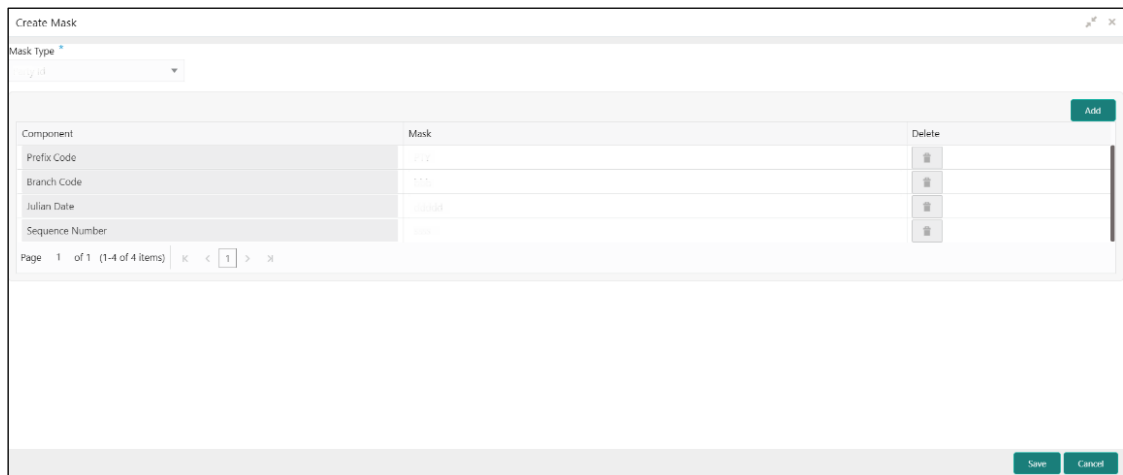
SSSS – Sequence Number

To Initiate Mask Code Maintenance

1. From **Home screen**, click **Party Services**. Under **Party Services**, click **Maintenance**.
2. Under **Maintenance**, click **Mask**. Under **Mask**, click **Create Mask**.

→ The **Create Mask** screen is displayed.

Figure 11: Create Mask



3. On **Create Mask** screen, specify the following attributes.

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

Table 9: Create Mask – Field Description

Field	Description
Mask Type	Select the mask type as Party Id from the dropdown list.
Component	Displays the attribute name added from the list.

Field	Description
Mask	<p>Specify the total length of the mask, which is the sum of length of all the attributes in the mask cannot exceed 36 characters.</p> <p>If no mask is defined, a default mask – PTYddddssss is applicable which includes:</p> <ul 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** 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.

Once the record is authorized by the checker,

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 is displayed.

Figure 12: View Mask



3 List of Menus

1. Customer Access Group - [Customer Access Group](#) (p. 4)
2. Entity Maintenance - [Entity Maintenance](#) (p. 11)
3. Location Maintenance - [Location Maintenance](#) (p. 13)
4. Mask Maintenance - [Mask Maintenance](#) (p. 15)
5. PII Masking Maintenance - [PII Masking Maintenance](#) (p. 6)