

Oracle® Banking Accounts Cloud Service

Party Configurations User Guide



Release 14.6.0.0.0
F78584-01
December 2022



Copyright © 2022, 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	iv
Related Documents	iv
Acronyms and Abbreviations	iv
List of Topic	v
Symbols and Icons	v
Basic Actions	v
Screenshot Disclaimer	vi

1 Configurations

1.1 Customer Access Group	1-1
1.2 PII Masking Maintenance	1-2
1.3 Entity Maintenance	1-7
1.4 Location Maintenance	1-8
1.5 Mask Maintenance	1-9

Index

Preface

This topic contains the following subtopics:

- [Audience](#)
- [Related Documents](#)
- [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*

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.

Table 4 (Cont.) Basic Actions

Action	Description
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:

- [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.
- [Entity Maintenance](#)
This topic describes the systematic instructions to initiate and view the Entity maintenance.
- [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.

1.1 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 1-1 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**.

1.2 PII Masking Maintenance

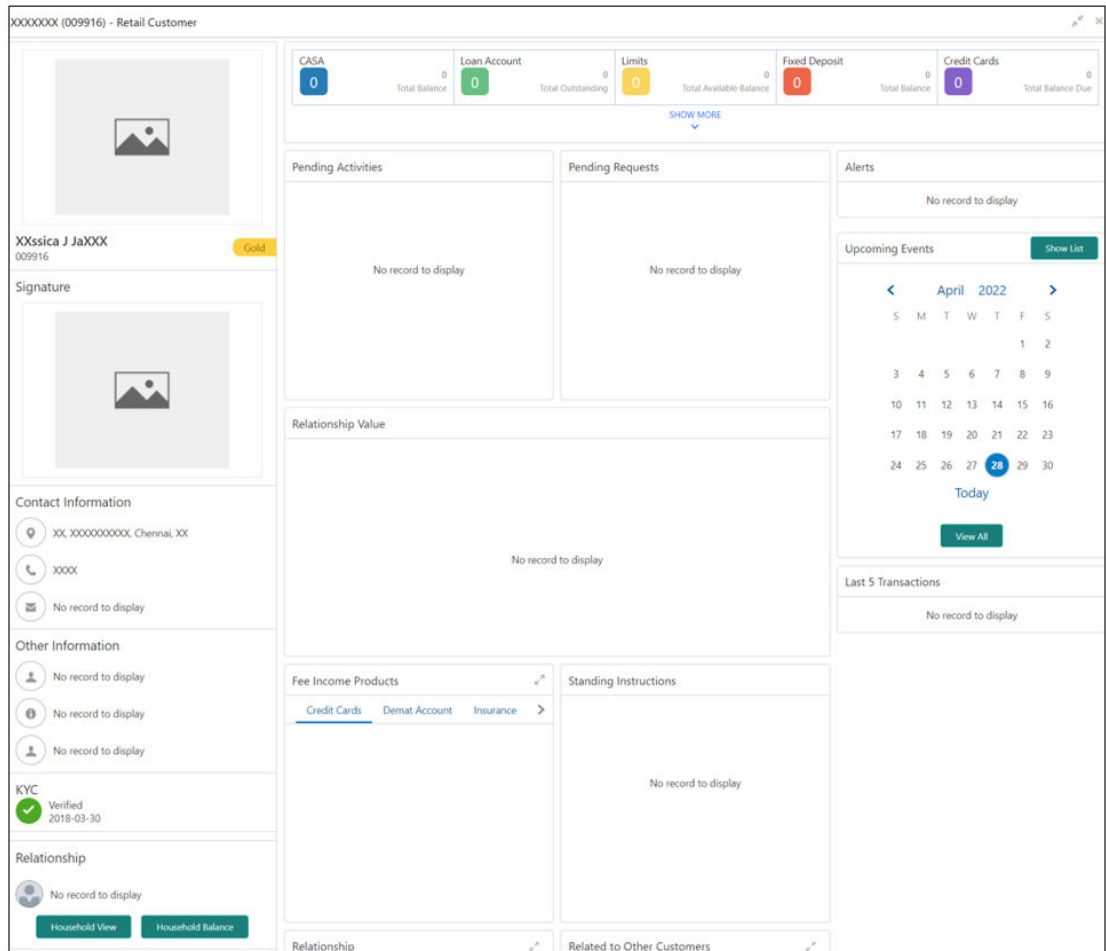
This topic describes the systematic instructions to initiate and view the PII Masking configurations.

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 1-1 Sample Masked Information



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

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 1-2 View and Update PII Mask



3. Click **Unlock**.

The **Create PII Mask** screen displays.

Figure 1-3 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.

Table 1-2 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 1-4 Edit PII Masking

The screenshot shows a window titled "Edit PII Masking". It contains a form with the following fields and values:

- Attribute Name: Title
- Data Type: String
- Data Length: 36
- Mask Enable:
- Mask Character: X
- Mask Entire Field:
- First N Characters: 0
- Last N Characters: 0

At the bottom right, there are two buttons: "Update" and "Cancel".

- 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 1-3 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.

7. 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 1-5 View and Update PII Mask



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

The **View PII Mask** screen displays.

Figure 1-6 View PII Mask



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 1-7 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.
Sub Entity Code	Specify the Sub Entity Code for the selected Entity Code.
Sub Entity Description	Specify the description of Sub Entity Code.

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

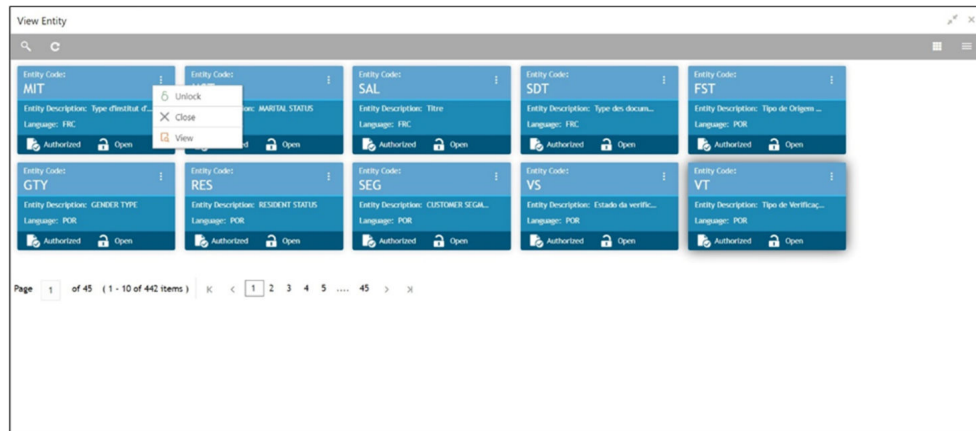
View Entity Maintenance

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

The **View Entity** screen displays.

Figure 1-8 View Entity



1.4 Location Maintenance

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

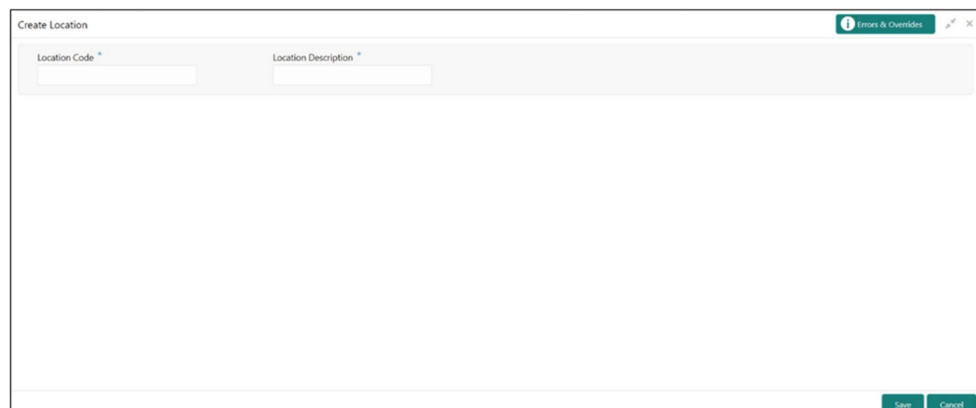
Location Maintenance enables the user to add, delete and modify Location Codes. Location Codes can be captured during party onboarding and amendment process to identify precise location of the customer. Location codes can be specific definition of locations within a specified area by the financial institutions.

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 1-9 Create Location



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

Table 1-5 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.

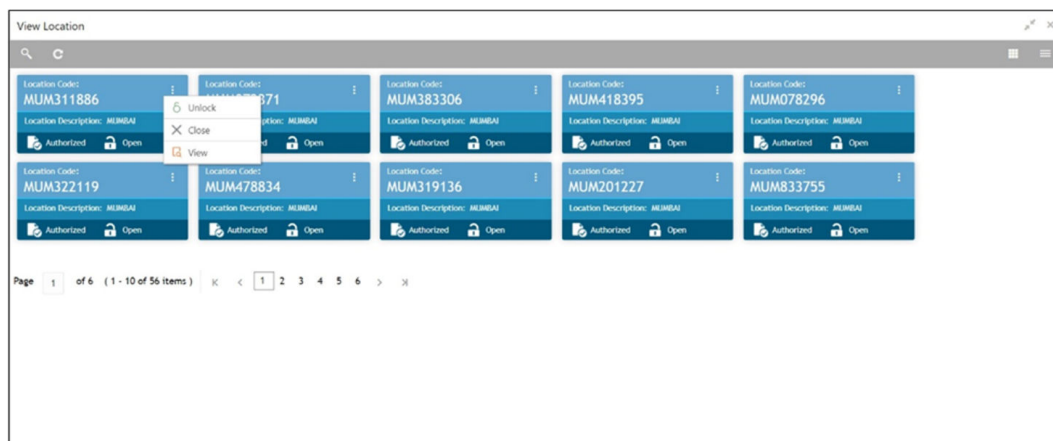
- Click **Save** to save the location code.

View Location Maintenance

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

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

Figure 1-10 View Location



1.5 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

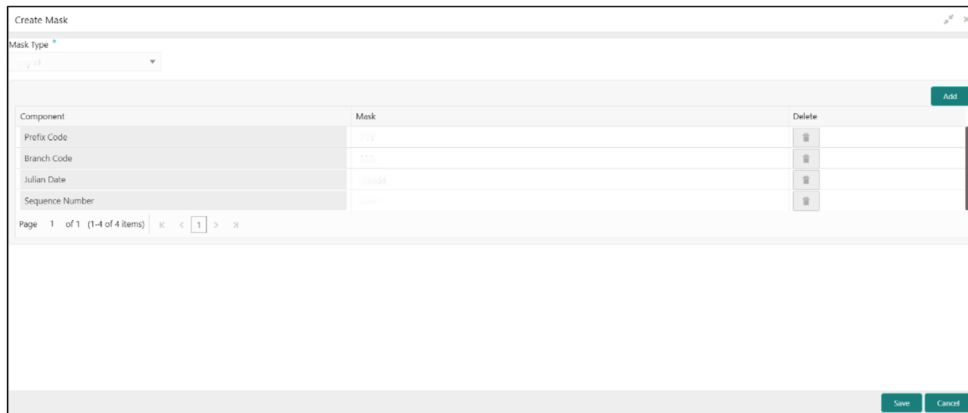
JJJ – Julian Date of current year

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 1-11 Create Mask



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

Table 1-6 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 1-12 View Mask



Index

C

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

E

Entity Maintenance, [1-7](#)

L

Location Maintenance, [1-8](#)

M

Mask Maintenance, [1-9](#)

P

PII Masking Maintenance, [1-2](#)