Oracle® Financial Services
Know Your Customer
Service Guide

Release 8.0.7.0.0
February 2021

ORACLE®

FINANCIAL SERVICES

ORACLE®

Oracle® Financial Services
Know Your Customer
Service Guide

Release 8.0.7.0.0
February 2021

Part Number: F17837-01

Revision History

The following table describes the revision history of the Service Guide.

Date	Edition	Description
February 2021	8.0.7.0.0	● Added a new service URL for customers who want the risk score of the primary customer to be inherited from the risk score of the related customer or customers in Onboarding Call Back Service Request Details.
December 2018	8.0.7.0.0	● Updated the Introduction to include content on KYC Onboarding. ● Added a new chapter, KYC Onboarding Service, which has information on the prerequisites to be done for Onboarding, the Onboarding process, and the web service names used in Onboarding. ● Added an Appendix, Configuring the Service Parameters through the User Interface, which contains the user interfaces used to configure the service parameters. ● Added a sample request JSON and a sample response JSON for KYC Onboarding in Sample JSONs for Onboarding Services. ● Removed chapters 3 and 4 from KYC Service Guide as they are not applicable for 807.
February 2019	8.0.7.0.1	● Updated the input and response JSONs in Sample JSONs for Onboarding Services.
March 2019	8.0.7.0.2	● Updated the response JSON in Sample JSONs for Onboarding Services. ● Updated the PMF workflow in KYC Onboarding Service.

Contents

Contents

About this Guide

The Oracle® Financial Services Know Your Customer (OFS KYC) Service Guide provides the details of the Onboarding service of the KYC application. The guide also contains the details of different processes used during the KYC Onboarding process.

This chapter focuses on the following topics:

- Who Should Use this Guide
- Scope of this Guide
- How this Guide is Organized
- Where to Find More Information

Who Should Use this Guide

This guide is intended for the technical staff, database programmers, and system administrators of the Oracle client.

Scope of this Guide

The purpose and scope of this guide is to provide details of the KYC Onboarding service. This guide covers all aspects of the service and the individual services made available as part of the KYC Onboarding service.

If you are using OFS KYC version 8.0.7, see *KYC Onboarding Service* and *Configuring the Service Parameters through the User Interface*.

For information on operating web services, see *Know Your Customer Service Guide* version 8.0.6.0.0. These chapters and services are also not applicable if you are using 8.0.7 but do not want to modify the Onboarding service integrations available in earlier versions.

How this Guide is Organized

The *Oracle Financial Services Know Your Customer Service Guide* includes the following chapters:

- *Introduction* provides a brief overview of the KYC Web Service.
- *KYC Onboarding Service* provides information on the prerequisites for KYC Onboarding, the KYC Onboarding process, and the web service names used in KYC Onboarding.
- *Sample JSONs for Onboarding Services* provides a sample input JSON and a sample response JSON for the Real-time Account Onboarding Risk (RAOR) and KYC Onboarding services.
- *Configuring the Service Parameters through the User Interface* provides information on configuring the KYC web services.

Where to Find More Information

For more information about Oracle Financial Services Know Your Customer, see the following documents available in the documentation library (*OHC*):

- *Oracle Financial Services Know Your Customer Risk Assessment Guide*

- *Oracle Financial Services Know Your Customer API Data Elements Guide*

- *Oracle Financial Services Know Your Customer Administrator Guide*

- *Oracle Financial Services Know Your Customer Service Guide*

To learn more about Oracle Financial Services and our complete product line, see our Web site www.oracle.com/financialservices.

Abbreviations Used in this Guide

This table lists the abbreviations used in this guide and their associated descriptions.

Table 1. Abbreviations Used in this Guide

Abbreviation	Description
AML	Anti-Money Laundering
T2T	Table to Table
AAI	Analytical Applications Infrastructure
OFS	Oracle Financial Services
BD	Behavior Detection
CS	Customer Screening
KYC	Know Your Customer
REST	Representational State Transfer
API	Application Program Interface

CHAPTER 1 *Introduction*

Customer Onboarding covers the different processes involved in the Onboarding of a Customer. The bank must ensure that they meet the global and local compliance regulatory requirements and ensure that the Customer Onboarding experience is smooth. As part of the internal KYC policy, banks collect additional compliance related information during Onboarding.

According to the regulations, the bank must collect all the required information from the Customer, perform identity verification and Customer Screening of the Customer, and evaluate the risk profile of the Customer before they decide whether the Customer can be Onboarded or not. The process is not just limited to the prospect who is opening an account or getting Onboarded, but is also applicable to all related parties like Joint Owners, Guardians, Directors, Signatories, and Beneficial Owners.

The Oracle Financial Service Know Your Customer (OFS KYC) application is a RESTful API service. The application has the following features:

- Allows all the compliance requirements to be met because of the integration with the Onboarding systems.

- Provides the Questionnaire capability, which is integrated with the Onboarding system. The Questionnaire output can be used during the Onboarding process.

- Integrates with multiple external sources for identity verification and screening of the Customers provided they are also RESTful services.

- Performs verification and screening for all the parties provided by the Onboarding system. Comes pre-integrated with the OFS Customer Screening (CS) product for screening the prospect and all the related parties.

- Configures the service must be called depending on the type of the applicant and the country where the verification must be performed.

KYC Onboarding Service

This chapter provides information on the Onboarding process and the web service names used in KYC Onboarding.

This chapter discusses the following topics:

- Onboarding Process Flow
- Invoking the KYC Onboarding Service
- Configuring/Modifying the PMF Flow for the Onboarding Service

Onboarding Process Flow

Before you begin the Onboarding process, ensure that Oracle Financial Services Analytical Applications (OFSAA) 8.0.7.0.0 and Behavior Detection (BD) 8.0.7.0.0 are installed and configured for KYC.

Even though the global requirements for KYC indicate what processes must be performed during Onboarding, the process flow for Onboarding differs from bank to bank. OFS KYC comes with a pre-defined Onboarding process covering all the major aspects of KYC compliance regulations. It also provides the flexibility to easily configure the workflow according to their requirement. The pre-defined Onboarding process has multiple ready-to-use sub-processes, which can be reused by all banks by providing the details of the external verification systems.
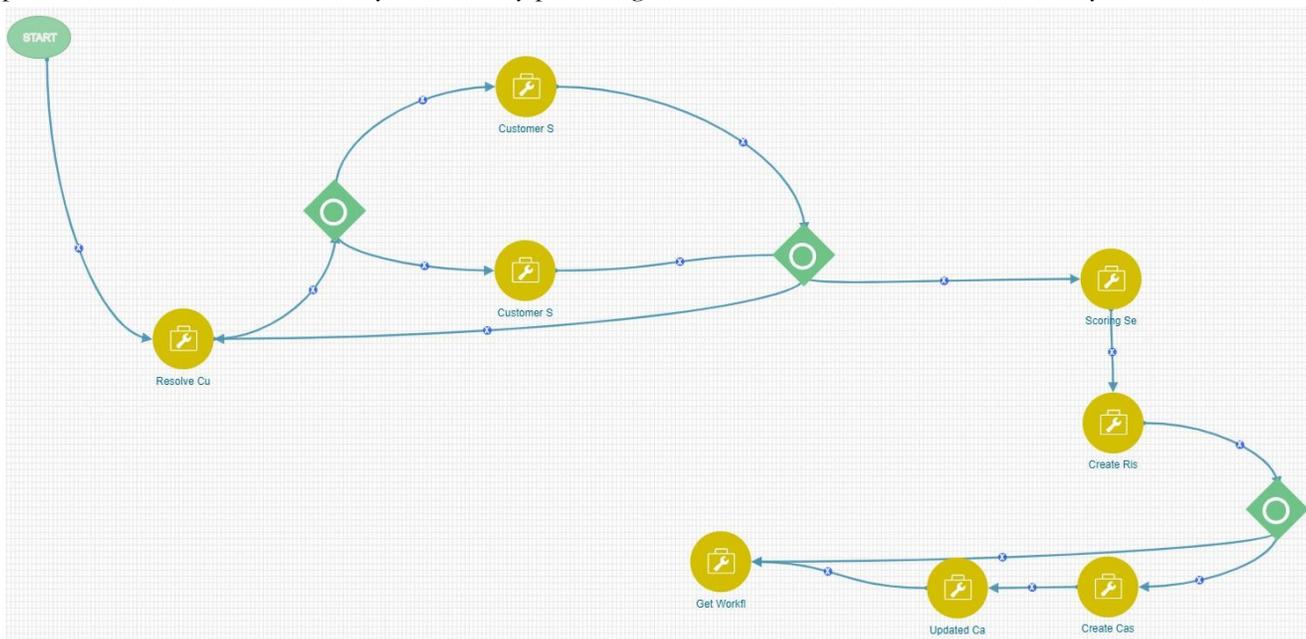
The Onboarding process includes the following steps:

1. **Workflow Access**: The ready-to-use workflow is available in the Process Modeller page in the Common Tasks menu. To access the workflow, see the *Getting Started* chapter in *Know Your Customer Administration Guide*.

    a. The service URLs must be provided in the following format:

    - For the scoring service: `http://#deployedserver#:#port#/RAOR/service/json/score`

◆ For the Customer screening service (individual):
```
http://#deployedserver#:#port#/edq/restws/Customer-Screening:IndividualScreen
```

◆ For the Customer screening service (non-individual):
```
http://#deployedserver#:#port#/edq/restws/Customer-Screening:EntityScreen
```

◆ For the watch list service:
```
http://#deployedserver#:#port#/#CONTEXTNAME#/CommonGatewayService/ComGtwy/initiateWatchlist
```

◆ For the create case service:
```
http://#deployedserver#:#port#/#CONTEXTNAME#/rest-api/CMRestService/RealTimeCaseCreationService/saveEventsAndPromoteToCase
```

2. **Resolve Customer**: Every party of an application must be verified and screened against the watch list. The decision to Onboard a prospect does not only depend on the prospect details but also on the details of the related parties of the prospect. The Onboarding system has the ability to divide every related party into sub-processes and do the processing of each sub-process.

3. **Watch list Screening:** The prospect and related parties must be screened against different watch lists to verify whether they belong to the watch list or not. This is a key criterion to decide the Onboarding process. OFS KYC is pre-integrated with Oracle Financial Services Customer Screening (OFS CS) and internal watch lists to perform this process. To enable or disable a screening process, see step 2, *Invoking the KYC Onboarding Service.*

4. **Identity Verification:** The integration process of Identity Verification is similar to the integration process of Customer Screening for RESTful API services. For other types of service integration, contact Oracle Support.

5. **Customer Scoring**: OFS KYC comes with a ready-to-use scoring model for the Onboarding service, which can be used to score a Customer with the available risk factors or score a Customer by adding more risk factors. The scoring service is the last service that must be called as this service uses the outputs of each of the above processes to arrive at the risk profile of the Customer. The ready-to-use Onboarding process converts the outputs of all individual services such as screening and identity verification into a risk factor.

6. **Risk assessment creation**: This is an internal process which creates the risk assessments for a request for audit purposes and, if required, for investigation. The users can also manually promote the risk assessments to cases from the user interface.

7. **Case creation service**: This service creates the cases for enhanced due diligence. The ready-to-use case criteria is defined as a decision rule in the Process Modelling Framework (PMF) workflow. Every range of risk category has a user review flag and an Onboard flag. The Onboarding system currently only assigns a user review flag for a risk category range. In the ready-to-use configuration, the case criteria are converted to a risk factor. In this way, the decision to create a case is determined by this configuration. A case is then created in Enterprise Case Management (ECM).

8. **Case ID creation**: After the case is created in ECM, the Onboarding system generates a task with a unique case ID against the risk assessment created.

Input Preparation/ Using the Individual Services/ Output Capture

The JSON inputs required for verification differs based on certain factors such as Customer type, jurisdiction, data sources, and external vendors. The JSON input preparation for each service is made configurable, transparent and flexible by the Table to JSON Utility. The output differs based on the above attributes. The output is used by the KYC system for risk scoring and is used for audit purposes. The JSON to Table Utility allows you to transform the JSON output into a table structure. For information on how to configure the utility, see *Know Your Customer Utilities Guide*.

The PMF work flow can be used to include the input, execution and output-related sub tasks in one process, which can be configured using the PMF User Interface. In PMF, these are termed as Pre Rule, Execution Rule and Post Rule.

The Pre Rule is used to define what data to pick for the input of each individual sub process. The Pre Rule is a URL of the Table to JSON utility for a specific mapping created to generate the JSON. For information on the Pre Rule mapping IDs, see *Know Your Customer Utilities Guide.*

The Execution Rule contains a placeholder for the Pre Rule URL to perform the task. For example, in Customer Screening, the Execution Rule is the URL of the OFS CS real time screening URL. For information on the URL formats used to invoke the service, see Step 1.

The Post Rule is used to define where the output data must be captured in the OFS KYC system. This is the JSON to Table URL for a specific mapping created to copy the output data into the KYC tables.

Deciding which Sub Process to Call

In most of the service integrations, the invoking process differs based on the attributes of the input and the output preparation. The Onboarding process is designed such that the service which must be used is selected. In PMF, this is called a *Decision Rule*. OFS KYC has leveraged this capability by defining filter conditions when a decision must be made. For example, OFS CS Individual tasks and OFS CS Non-Individual tasks use the decision rules that check the Customer type value of the JSON.

Invoking the KYC Onboarding Service

This section provides information on invoking the service and what happens after the service is invoked.

1. The Request Details, Response Details, and Response Status Details for the Onboarding service are shown:

Table 2. Request Details

Parameter Name	Parameter Value	Comments
Service URL	#HTTP_PROTOCOL#://#SERVER_NAME#:#SERVER_PORT#/InitiateOnboardingService/OB/Initiate	#HTTP_PROTOCOL#://#SERVER_NAME#:#SERVER_PORT are implementation specific and must be set during the installation process.
Method Type	POST	
Authorization	Basic Auth	A valid KYC administrator user ID and password must be passed.
Content-Type	application/json	To view a sample request JSON, see *KYC Onboarding Request JSON.* To view the details of the JSON, see the *Know Your Customer API Data Elements Guide.*

Table 3. Response Details

Parameter Name	Parameter Value	Comments

Response Content-Type	application/json	Sample Response:
		`{`
		`    "RequestID": 1001,`
		`    "applicationId": "CIF-200050799"`
		`}`

Table 4. Response Status Details

Response Status Codes	Status Description	Comments

Status 200	Request taken up for processing	Sample Response:
		
		``
		{
		    "RequestID": 1001,
		    "applicationId": "CIF-200050799"
		}
		``

Status 401	Request Unauthorized	Sample Response:
		
		``
		{
		    "ERROR - ": "Authentication failed in Initiate Onboarding"
		}
		``

Status 400	Incorrect input JSON structure	Sample Response:
		
		``
		{
		    "ERROR - ": "JSON input provided is blank/incorrect"
		}
		``

Status 400	Mandatory elements are not provided in the Input JSON	Sample Response:
		
		``
		{
		    "ERROR - ": "Either requestUserId or applicationId are not provided. Please provide the same and retry"
		}
		``

Status 500	Mis-match in data lengths	Sample Response:
		
		``
		{
		    "ERROR: ": "SQL Error Occurred While Saving Data In FCC_OB_REQUEST:java.sql.SQLException: ORA-12899: value too large for column \"UT_ATOM\".\"FCC_OB_REQUEST\".\"APPLICATION_ID\" (actual: 1008, maximum: 255)\n"
		}
		``

If any errors are generated, the error message is sent back as a response with the error details mentioned. The errors must be corrected and the input JSON must be resubmitted with the required corrections made to the Onboarding service.

Note: Every submission is considered as a new request by the system.

2. Following the successful invocation of the Onboarding service, the request is acknowledged with a unique request ID and the application ID. The Request ID can be used as a reference to:

   ■ Track the process in the Process Monitor page. For more information, see Monitoring the Process in the Process Modelling Framework (PMF).

   ■ Get the overall response from the Onboarding service once the Onboarding process is completed.

■ Perform the due diligence in KYC and ECM.

3. The Onboarding Callback service, as part of its response, provides the details of the specific Request ID in the JSON format. The details of the Onboarding Callback service and the JSON elements are in Table 5. To get the overall response from the Onboarding service for a request, you must configure a new Task in PMF at the end of the `KYC_ONBOARDING` workflow to call your service which accepts a JSON as input and in the format generated by the Onboarding call back service.

To configure a task in PMF:

a. Create a new service task at the end of the `KYC_ONBOARDING` workflow.

   i. Configure the Onboarding call back service as a `Pre Rule`.

   ii. Configure your service as an `Execution Rule` and pass the output of the `Pre Rule` to this `Execution Rule`.

This ensures that the overall Onboarding response is updated in the source/invoking system at the end of the process.

Table 5. Onboarding Call Back Service Request Details

Parameter Name	Parameter Value	Comments
Service URL for primary customers who do not want risk to be inherited from the related customers	#HTTP_PROTOCOL#://#SERVER_NAME#:# SERVER_PORT#/TabletoJSONService/TableToJson/createtabletojson?mappingId=OB_RESP_1&requestId=#REQUEST_ID#	#HTTP_PROTOCOL#://#SERVER_NAME#:#SERVER_PORT are implementation-specific and these are set during the installation process. #REQUEST_ID# must be replaced with RequestID received as part of the Onboarding Service Response.
Service URL for primary customers who want risk to be inherited from the related customers	#HTTP_PROTOCOL#://#SERVER_NAME#:#SERVER_PORT#/TabletoJSONService/TableToJson/createtabletojson?mappingId=KYCOB_RESP_1&requestId=#REQUEST_ID#	#HTTP_PROTOCOL#://#SERVER_NAME#:#SERVER_PORT are implementation-specific and these are set during the installation process. #REQUEST_ID# must be replaced with RequestID received as part of Onboarding Service Response.
Method Type	POST	NA
Authorization	Basic Auth	A valid KYC administrator user ID and password must be used.

Table 6. Onboarding Call Back Service Response Details

Parameter Name	Parameter Value	Comments
Response Content-Type	application/json	To view a sample response JSON, see *KYC Onboarding Response JSON*.

Monitoring the Process in the Process Modelling Framework (PMF)

Use the PMF page to view all processes which are triggered for a particular request ID.

To access the Process Monitor page:

1. Login as the KYC Administrator.

2. Click the **Process Modelling Framework** icon and then select **Process Monitor**.

3. In the *Process Monitor* page, click the request ID link for which you want to view the triggered processes.

A completed sub-process is marked with ✅.

If an error is displayed in the Process Monitor page against any task, check the server logs for further details on the error:

- For a Tomcat server, the path is

  `tomcat -/scratch/ofsaaapp/apache-tomcat-8.0.30/webapps/BD807KYC/logs`

- For a Weblogic server, the path is
  `/scratch/ofsaebas/Oracle/Middleware/Oracle_Home/user_projects/domains/KYC8071510/appl ications/KYC8071510.ear/KYC8071510.war/logs`

Configuring/Modifying the PMF Flow for the Onboarding Service

When you configure the ready-to-use PMF flow, you must:

1. **Create the new PMF flow**: Take a copy of the ready-to-use PMF flow provided and modify it as required. This ensures that all ready-to-use features are also available in the new flow diagram.

2. **Add an Identity Verification (IDV) Process**: You can configure the IDV process with an external vendor if the vendor is offering a rest-based service. Use the Table to JSON utility to configure the process. For more information, see *Know Your Customer Utilities Guide*.

   The information required by most of the vendors for IDV differ on certain attributes. To do the necessary configurations, perform the same tasks which are defined for the ready-to-use OFS CS. You must also define the Pre Rule, Execution Rule and Post Rule as per OFS CS.

3. **Enable the internal watch list/OFS CS**: Depending on the watch list used, the configurations and data loading must be done, and either the internal watch list or the and OFS CS watch list must be configured.

Note:

- This is applicable only if you have integrated KYC with Customer Screening. For information on configuring the watch lists used by the KYC system, see *Customer Screening Administration and Configuration Guide*.

- If you are using an internal watch list, that is, a watch list used by your bank, ensure that all internal watch list data is loaded.

The Customer Screening web service is executed by default. To enable the internal watch list web service:

   i. Login as the KYC Administrator.

   ii. Click the **Process Modelling Framework** icon and then select **Process Modeller**.

   iii. In the **Process Modeller** page, click the **KYC_ONBOARDING** link.

   Note: To view this link, ensure that you have mapped the KYC Administrator user to the KYC Administrator user group.

   iv. In the PMF screen, delete the flow lines corresponding to the Customer Screening watch list by clicking ⊠ on the flow line.

   v. To add the internal watch list web service, first click the service task activity and then click anywhere in the PMF flow.

   vi. Drag and drop the **Activity** icon 🕑 to the required location.

   vii. Double-click the **Activity** icon and provide an Activity name.

   viii. Double-click the **Implementation** icon ⚙ . The Implementation menu appears.

   ix. In the **Implementation** menu, select the **Execution Rule** as `OFSS Watch List URL` and click **OK**. To edit the rule, click the `OFSS Watch List URL` link.

      x. In the **Implementation** menu, select the **Pre Rule** as `Persist Response as OFSS Watch  List` and click **OK**. To edit the rule, click the `Persist Response as OFSS Watch List` link.

     xi. Close the PMF screen.

4. **Add a different RESTful screening process**: If the client has a different RESTful screening process, then you can perform the same steps as defined for OFS CS.

5. **Call Back Service**: The call back service is used to get the overall response for the Onboarding service. For more information, see step 3, Invoking the KYC Onboarding Service.

    Note: The Scoring Service, Risk Assessment creation, Case creation, and Update Case ID related tasks do not require any modifications unless a new data field must be added to the case management system.

APPENDIX A   *Sample JSONs for Onboarding Services*

This appendix contains a sample input and response JSON for the Real-time Account Onboarding (RAOR) and Onboarding services. Both the input and response JSONs have the complete list of data elements available in the product. See *Know Your Customer API Data Elements Guide* for information on each data element, the accepted values for each data element, and their usage.

The input JSON is the expected input for the Onboarding service. Depending on the data elements that you require, you can configure the JSON structure. As a part of this exercise, ensure that the JSON structure is valid. The sample JSONs provided in *MOS* contain all data elements as defined by the product. For information on the JSON structure, see *Know Your Customer API Data Elements Guide*.

The response JSON is generated by the system after the Onboarding process is completed. This has the complete data elements of each individual sub process. Depending on the requirement, the required data elements for a response can be configured using the Table to JSON utility. For more information, see *Know Your Customer Utilities Guide*.

NOTE: Changes to the JSON structure are not allowed.

APPENDIX B

Configuring the Service Parameters through the User Interface

The following UIs are used to configure the service parameters of the KYC Onboarding services. This must be done so that the Onboarding system knows the service parameter values which must be used during the Onboarding process.

- Configuring the Onboarding Service Parameters
- Configuring the Common Gateway Service Parameters

Configuring the Onboarding Service Parameters

Use the Configure Service Parameters UI to configure the service URL, service user name, and service password for all services.

The service URLs are pre-populated during the installation process with content from the `InstallConfig.xml` file. If the deployment URL is not mentioned during installation, or if the deployment URL has changed after installation, you must provide the new service URL.

The service user name and password must be updated for all services except the AAI Authorization Service.

Note:

- Ensure that all service user names and service passwords provided are of valid OFSAA KYC Administrator users.
- For the ECM Case Creation URL service, the service user name and service password provided must be of a valid OFSAA ECM Administrator user.

To view the UI:

1. Log in to the KYC application as the KYC Administrator. For more information, see the *Getting Started* chapter in the *Know Your Customer Administrator Guide*.

2. From the **Behavior Detection** menu, select **KYC,** then select **Manage KYC OB Configuration**, and then select **Configure Service Parameters**.
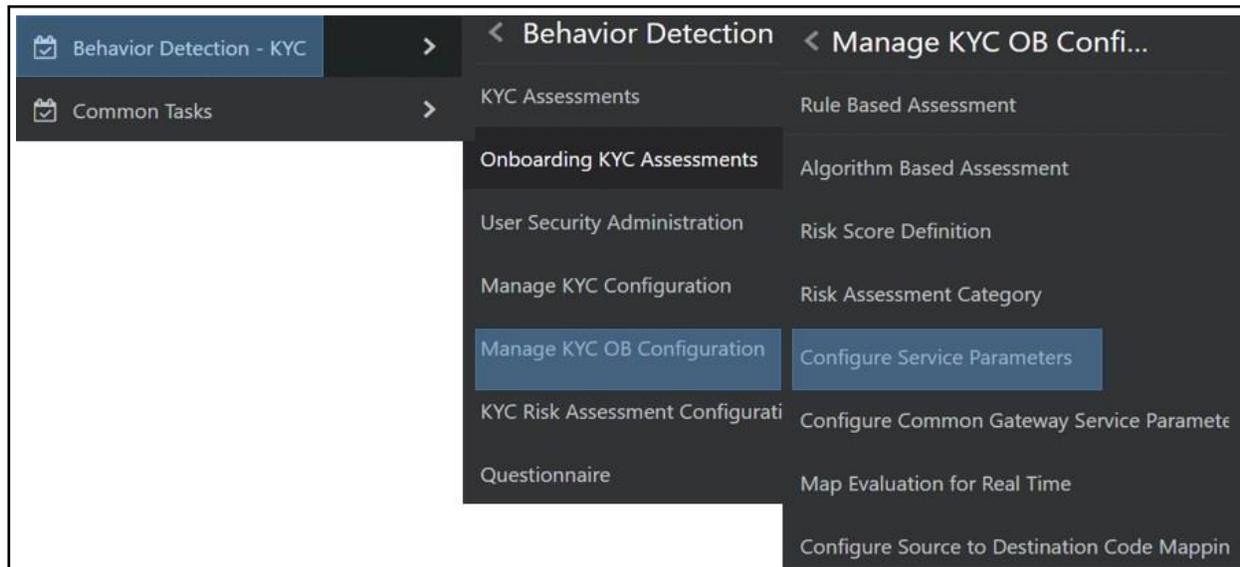
The Configure Service Parameters UI appears. You can select one of the following services:

- **AAI Authorization Service**
- **Initiate OB URL**
- **Process Modeling Framework Service**
- **Table to JSON Mapping Utility**
- **ECM Case Creation URL**
- **Generate Case Input URL**
- **Common Gateway Service URL**

Modifying the Web Service Parameter Details

To modify the web service parameters:

1. In the **Service Name** field, select the web service for which you want to edit the service parameters.

2. Update the service URL if the deployment URL is not mentioned during installation, or if the deployment URL has changed after installation.

3. Update the service user name and password.

4. Click **Save** to save the details.

The Edit Service Parameters section is applicable only for the Process Modeling Framework service.

The three applicable parameters and their corresponding values are:

- PMF_PROCESS: KYC_ONBOARDING

- INFODOM: Installation Specific

- LOCALE: en_US

All the three parameters are pre-populated and should be changed only if there is a change in these values post installation.

Configuring the Common Gateway Service Parameters

Use the Common Gateway Service Parameters UI to edit the service parameters related to the common gateway service.

To view the UI:

1. Log in to the KYC application as the KYC Administrator. For more information, see the *Getting Started* chapter in the *Know Your Customer Administrator Guide*.

2. From the **Behavior Detection** menu, select **KYC**, then select **Manage KYC OB Configuration**, and then select **Configure Common Gateway Service Parameters**.
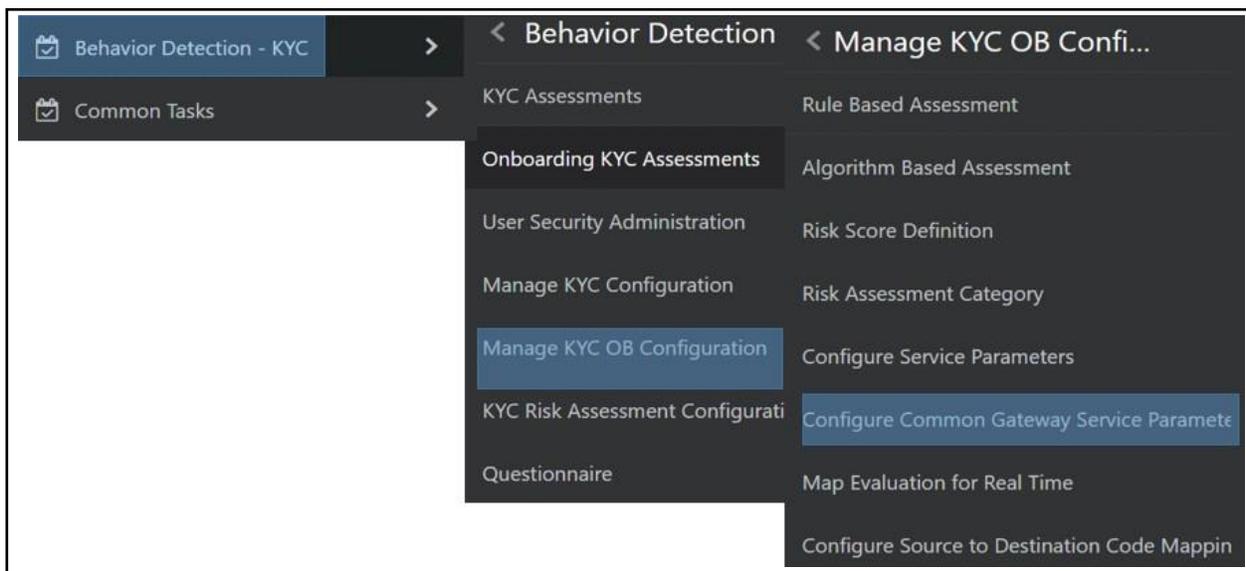
The Configure Common Gateway Service Parameters UI appears. You can select one of the following services:

- **AAI Authorization Service**

- **Internal Watch List Service**

● **Process Modeling Framework**

Modifying the Web Service Parameter Details

To modify the web service parameters:

1. In the **Service Name** field, select the web service for which you want to edit the service parameters.

2. Update the service URL if the deployment URL is not mentioned during installation, or if the deployment URL has changed after installation.

3. Update the service user name and password except for the AAI Authorization Service.

4. Click **Save** to save the details.

Note: After you make the above changes, restart the web server.

Adding New Field in KYC Onboarding JSON Request

To add a new field in KYC OB Request JSON, follow these steps:

1. Open the `KYCOBrequestJsonSchema.json` file in the `$FIC_HOME/Onboarding/InitiateOnboardingService/WEB-INF/classes` path. Replace the `{new_field_business_name}` placeholder value in the following script under the properties tag.

```
"{new_field_business_name}": {

        "$id":
"#/properties/OnboardingCustomer/properties/{new_field_business_name}",

        "type": "string",

        "title": "The {new_field_business_name}
Schema",

        "default": "",

        "examples": [

                ""

        ],

        "maxLength": 1
```

```
}
```

2. Create a column in the `FCC_OB_CUST` table.

> Example: `CUSTOM_FLAG_COLUMN_NAME`

> **NOTE**   Make sure to take a backup of `FCC_OB_CUST` table when any official patch is getting applied.

3. Replace the `{CUSTOM_FLAG_COLUMN_NAME}`and `{new_field_business_name}` placeholder values in the following script and execute it in the Atomic schema.

```
MERGE INTO FCC_OB_PHY_BUS_COL_NM_MAP T USING (

SELECT 'FCC_OB_CUST' TABLE_NAME, '{CUSTOM_FLAG_COLUMN_NAME}'
COLUMN_NAME, '{new_field_business_name}' BUSINESS_NAME, 'STRING'
COLUMN_TYPE, '' COLUMN_LENGTH FROM DUAL) S

ON ( T.TABLE_NAME = S.TABLE_NAME AND T.COLUMN_NAME = S.COLUMN_NAME )

WHEN MATCHED THEN UPDATE SET T.BUSINESS_NAME = S.BUSINESS_NAME,
T.COLUMN_TYPE = S.COLUMN_TYPE, T.COLUMN_LENGTH = S.COLUMN_LENGTH

WHEN NOT MATCHED THEN INSERT

(TABLE_NAME,COLUMN_NAME,BUSINESS_NAME,COLUMN_TYPE,COLUMN_LENGTH)

VALUES

(S.TABLE_NAME,S.COLUMN_NAME,S.BUSINESS_NAME,S.COLUMN_TYPE,S.COLUMN_L
ENGTH)

/
```

4. Execute the ant.sh file in the $FIC_HOME/Onboarding path.

5. Stop the OFSAA Services.

6. Create the `InitiateOnboardingService` EAR/WAR file and redeploy this new war on the web application server. Refer the Behavior Detection Installation Guide for the steps related to deployment.

7. Restart the OFSAA services.

Index

Index