Oracle Financial Services Know Your Customer

Service Guide

Release 8.1.2.2.0

September 2022

F17837-03

ORACLE®
Financial Services

OFS Know Your Customer Service Guide

Document Control

Table 1: Document Control

Version Number	Revision Date	Change Log
8.1.2.2.0	September 2022	Added the details regarding “SyncAPIFlag” in the Onboarding Process Flow section.
8.1.2.1.0	June 2022	A new version has been created for the 8.1.2.1.0 release.
8.1.2.0.0	March 2022	Updated the Response Status Details table in the Configuring/Modifying the PMF Flow for the Onboarding Service section.
8.1.1.0.0	July 2021	Created the document.

Table of Contents

1 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.

1.1 Who Should Use This Guide

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

1.2 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.
- Appendix A: 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.
- Appendix B: Configuring the Service Parameters through the User Interface provides information on configuring the KYC web services.

1.3 Where to Find More Information

For more information about Oracle Financial Services KYC, see the following documents:

- **Know Your Customer Administration Guide**
- **Know Your Customer Risk Assessment Guide**
- **Data Interface Specification (DIS) Guide**
- **Data Model Reference (DMR) Guide**
- **API Data Elements Guide**
- **Utilities Guide**
- **Enterprise Case Management User Guide**

These documents can be found at the following link: https://docs.oracle.com/cd/E91253_01/kycguides.htm.

To find additional information about how Oracle Financial Services solves real business problems, see our website at www.oracle.com/financialservices.

1.4 Conventions Used in This Guide

Table 1 mentions the conventions used in this guide.

Table 1: Conventions Used

Conventions	Meaning
Italics	Names of books as references Emphasis Substitute input values
Bold	Menu names, field names, options, button names Commands typed at a prompt User input
`Monospace`	Directories and subdirectories File names and extensions Code sample, including keywords and variables within the text and as separate paragraphs, and user-defined program elements within the text
Hyperlink	Hyperlink type indicates the links to external websites and internal document links to sections.
Asterisk (*)	Mandatory fields in User Interface
<Variable>	Substitute input value

2 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, and evaluate the Customer's risk profile before deciding whether the Customer can be Onboarded. 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:

- All compliance requirements must 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.
- It 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 applicant and the country where the verification must be performed.

3 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

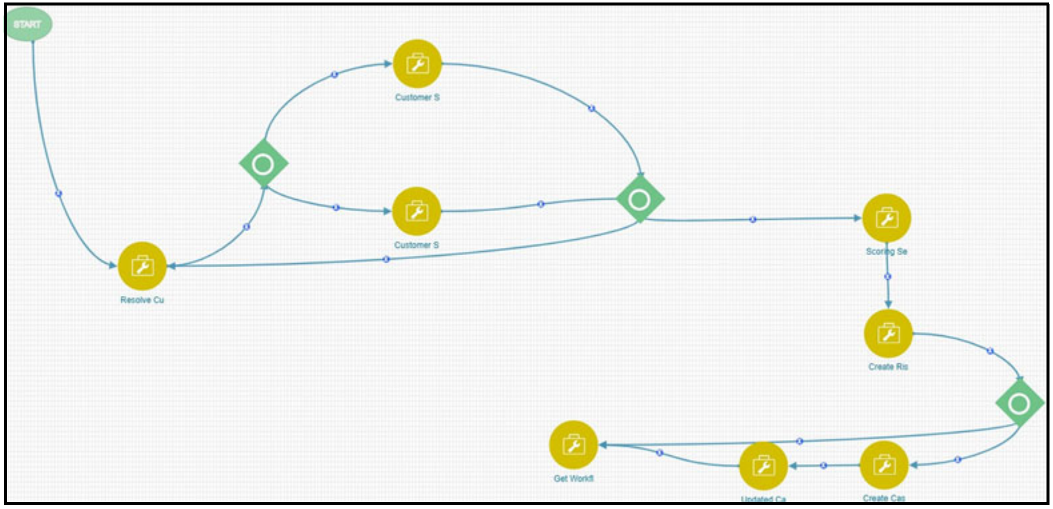
3.1 Onboarding Process Flow

Before you begin the Onboarding process, ensure that Oracle Financial Services Analytical Applications (OFSAA) 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 allows the flexibility to easily configure the workflow according to their requirements. The pre-defined Onboarding process has multiple ready-to-use sub-processes, which all banks can reuse by providing the details of the external verification systems.

KYC Onboarding has defined the API request data elements by considering the different processes to be conducted during onboarding. KYC supports both synchronous and asynchronous API for Real-time Risk Assessment from 8.1.2.0.0 onwards. A new JSON attribute, " SyncAPIFlag," has been added to the request data elements. For synchronous calls, pass the value as “Y” else “N.”

Figure 1: Onboarding Process Flow



The Onboarding process includes the following steps:

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

   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/in itiateWatchlist
```

- For the create case service:

```
http://#deployedserver#:#port#/#CONTEXTNAME#/rest-api/CMRestService/
RealTime CaseCreationService/saveEventsAndPromoteToCase
```

2. **Resolve Customer**: Every party of an application must be verified and screened against the watch list. The decision to Onboard a prospect depends not only on the prospect's details but also on the details of the related parties of the prospect. The Onboarding system can 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 My Oracle Support (MOS).
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 Customer's risk profile. 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 that 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 cases for enhanced due diligence. The ready-to-use case criteria are 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.

3.1.1 Input Preparation/ Using the Individual Services/ Output Capture

The JSON inputs required for verification differ based on 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 KYC system uses the output 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 configuring the utility, see Oracle Financial Services Know Your Customer Utilities Guide.

The PMF workflow 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 subprocess. 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 Oracle Financial Services 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 Invoking the KYC Onboarding Service.

The Post Rule defines 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.

3.1.2 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 to select the service that must be used. 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.

3.2 Invoking the KYC Onboarding Service

This section provides information on invoking the service and what happens after the service is invoked. The Request Details, Response Details, and Response Status Details for the Onboarding service are shown in Table 2, Table 3, Table 4, Table 5, and Table 6:

Table 2: Request Details

Parameter Name	Parameter Value
Service URL	#HTTP_PROTOCOL#://#SERVER_NAME#:#SERVER_PORT#/InitiateOnboardingService/OB/Initiate
Method Type	POST
Authorization	Basic Auth
Content-Type	application/json

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	The 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 request user id or application Id are not provided. Please provide the same and retry"
		}

Table 4: Response Status Details

Response Status Codes	Status Description	Comments
Status 400	Invalid attributes in the Input JSON.	Sample Response: [#/properties/OnboardingCustomer/properties/PrimaryCustomer : abcd does not match the allowed regex pattern (^[Y]$).]

Status 500	Mis-match in data lengths	Sample Response:
		{
		"ERROR: ": "SQL Error Occurred While Saving Data In FCC_OB_REQUEST:java.sql.SQLExcep tio n: ORA-12899: value too large for column
		\"UT_ATOM\".\"FCC_OB_REQUEST\".\"AP PLICATION_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 a new request by the system.

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 on 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.

The Onboarding Callback service, as part of its response, provides the details of the specific Request ID in 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 calls back service.

To configure a task in PMF, follow these steps:

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

2. Configure the Onboarding call back service as a Pre Rule.
3. 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	#HTTP_PROTOCOL#:// #SERVER_NAME#:# SERVER_PORT#/TabletoJSONService/ TableToJ son/ createtabletojson?mappingId=KYCOB_RESP_1&re questId=#REQUEST_ID#	#HTTP_PROTOCOL#:// #SERVER_NAME#:#SE RVER_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.
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.

4. Monitor the Process in the Process Modelling Framework (PMF). Use the PMF page to view all processes triggered for a particular request ID. To access the Process Monitor page:
   a. Log in as the KYC Administrator.
   b. Click the **Process Modelling Framework** icon and then select **Process Monitor**.
   c. On the Process Monitor page, click the request ID link for which you want to view the triggered processes.
   d. A completed sub-process is marked with ✓.
   e. 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/applications/KYC8071510.ear/KYC8071510.war/logs
```

3.3 Configuring/Modifying the PMF Flow for the Onboarding Service

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

- **Create the new PMF flow**: Take a copy of the ready-to-use PMF flow and modify it as required. This ensures that all ready-to-use features are available in the new flow diagram.
- **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 Oracle Financial Services Know Your Customer Utilities Guide.

  The information required by most of the vendors for IDV differs on specific attributes. To do the necessary configurations, perform the same tasks defined for the ready-to-use OFS CS. You must also define the Pre Rule, Execution Rule, and Post Rule as per OFS CS.
- **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 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 Oracle Financial Services 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, follow these steps:

a. Log in as the KYC Administrator.

b. Click the Process Modelling Framework icon and then select Process Modeller.

c. On 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.

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

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

f. Drag and drop the Activity icon ↻ to the required location.

g. Double-click the Activity icon and provide an Activity name.

h. Double-click the Implementation icon ⚙ . The Implementation menu appears.

i. 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.

j. 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.

k. Close the PMF screen.

- **Add a different RESTful screening process**: If the client has a different RESTful screening process, then you can perform the same steps defined for OFS CS.
- **Call Back Service**: The callback 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.

4 Appendix A: Sample JSONs for Onboarding Services

WARNING Do not make any changes to the JSON structure.

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. For information on each data element, the accepted values for each data element, and their usage, see Oracle Financial Services Know Your Customer API Data Elements Guide.

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 defined by the product.

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

5 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 used during the Onboarding process.

- Configuring the Onboarding Service Parameters
- Configuring the Common Gateway Service Parameters
- Adding New Field in KYC Onboarding JSON Request

5.1 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.

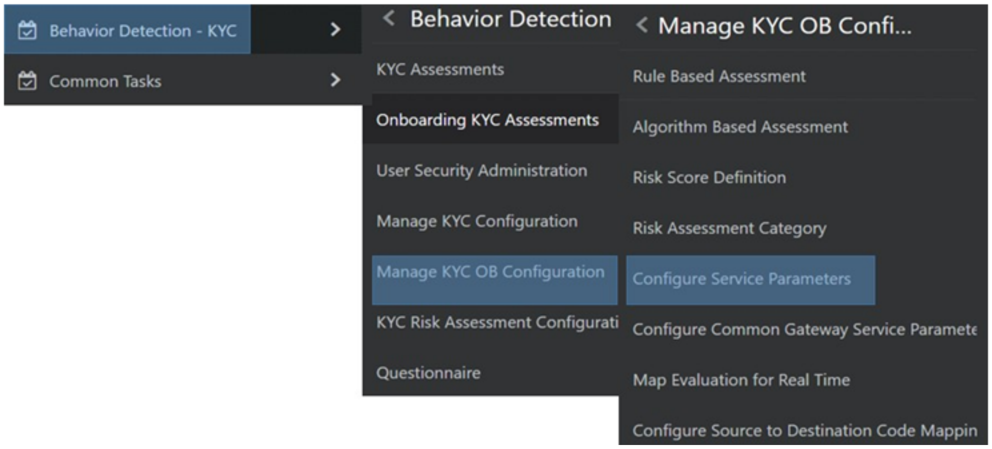
If the deployment URL is not mentioned during installation, or if the deployment URL has changed after installation, you must provide the new service URL. The service user name and password must be updated for all services except the AAI Authorization Service.

> **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, follow these steps:

1. Log in to the KYC application as the KYC Administrator. For more information, see the *Getting Started* chapter in the Oracle Financial Services Know Your Customer Administrator Guide.
2. From the Behavior Detection menu, select **KYC**, select **Manage KYC OB Configuration**, and then select **Configure Service Parameters**.

Figure 2: Navigation


Behavior Detection - KYC
Common Tasks
Behavior Detection
KYC Assessments
Onboarding KYC Assessments
User Security Administration
Manage KYC Configuration
Manage KYC OB Configuration
KYC Risk Assessment Configurati
Questionnaire
Manage KYC OB Confi...
Rule Based Assessment
Algorithm Based Assessment
Risk Score Definition
Risk Assessment Category
Configure Service Parameters
Configure Common Gateway Service Paramete
Map Evaluation for Real Time
Configure Source to Destination Code Mappin

The Configure Service Parameters UI appears. You can select one of the following services:

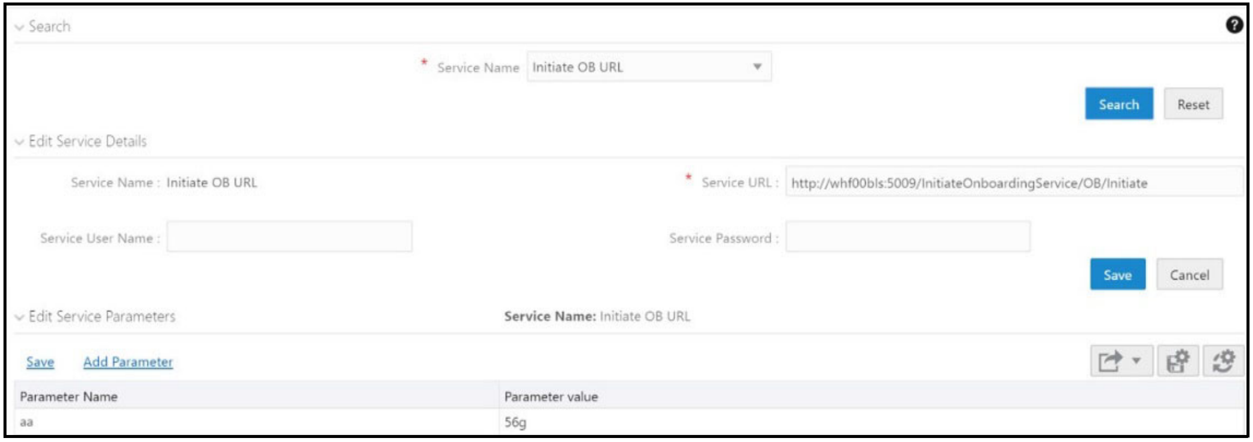
- **AAI Authorization Service**
- **Initiate OB URL**

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

5.1.1 Modifying the Web Service Parameter Details

To modify the web service parameters, follow these steps:

Figure 3: Onboarding Service Parameters



Search

* Service Name: Initiate OB URL

Edit Service Details

Service Name : Initiate OB URL

* Service URL : http://whf00bls:5009/InitiateOnboardingService/OB/Initiate

Service User Name :

Service Password :

Edit Service Parameters

Service Name: Initiate OB URL

Parameter Name	Parameter value
aa	56g

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 S**ervice User Name** and **Service Password**.
4. Click **Save** to save the details.

The Edit Service Parameters section only applies to the Process Modeling Framework service. The three applicable parameters and their corresponding values are:

- PMF_PROCESS: KYC_ONBOARDING
- INFODOM: Installation Specific
- LOCALE: en_US

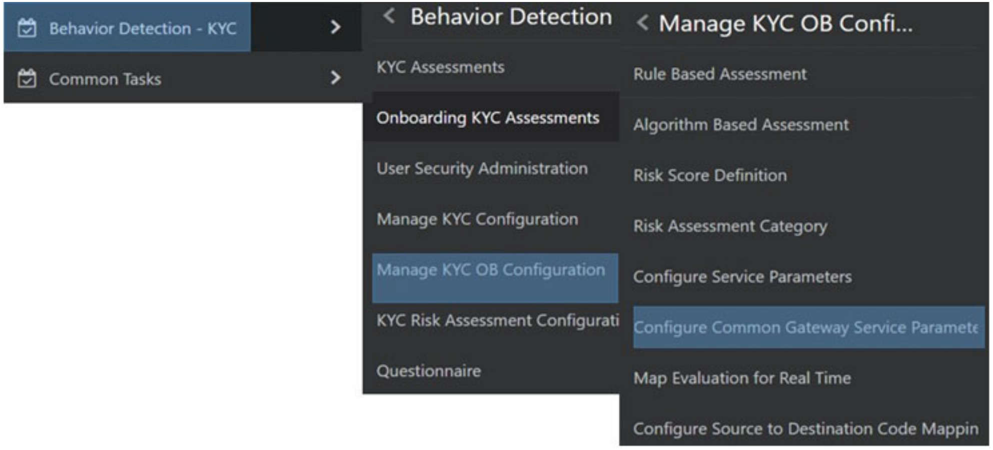
All three parameters are pre-populated and should be changed only if there is a change in these values post-installation.

5.2 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, follow these steps:

1. Log in to the KYC application as the KYC Administrator.
2. From the Behavior Detection menu, select **KYC**, select **Manage KYC OB Configuration**, and then select **Configure Common Gateway Service Parameters**.

Figure 4: Navigation


Behavior Detection - KYC
Common Tasks
Behavior Detection
KYC Assessments
Onboarding KYC Assessments
User Security Administration
Manage KYC Configuration
Manage KYC OB Configuration
KYC Risk Assessment Configurati
Questionnaire
Manage KYC OB Confi...
Rule Based Assessment
Algorithm Based Assessment
Risk Score Definition
Risk Assessment Category
Configure Service Parameters
Configure Common Gateway Service Paramete
Map Evaluation for Real Time
Configure Source to Destination Code Mappin

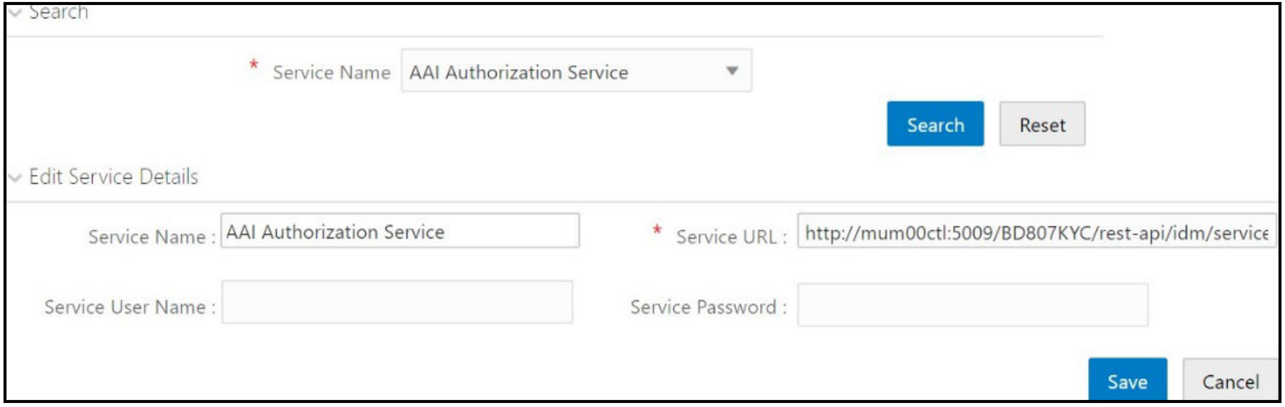
The Configure Common Gateway Service Parameters UI appears. You can select one of the following services:

- **AAI Authorization Service**
- **Internal Watch List Service**
- **Process Modeling Framework**

5.2.1 Modifying the Web Service Parameter Details

To modify the web service parameters, follow these steps:

Figure 5: Common Gateway Service Parameters



Search

* Service Name: AAI Authorization Service

Edit Service Details

Service Name : AAI Authorization Service

* Service URL : http://mum00ctl:5009/BD807KYC/rest-api/idm/service

Service User Name :

Service Password :

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.

5.3 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_LENGT
H)

/
```

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.

OFSAA Support

Raise a Service Request (SR) in My Oracle Support (MOS) for queries related to the OFSAA applications.

Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.